United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FORTINET, INC.,
Plaintiff,
v.
FORESCOUT TECHNOLOGIES, INC.,
Defendant.

Case No. 20-cv-03343-EMC

CLAIM CONSTRUCTION ORDER

I. INTRODUCTION

Fortinet, Inc. ("Fortinet") brought this action against Forescout Technologies, Inc. ("Forescout"), asserting infringement of five patents. Forescout counterclaimed with infringement of six of its own patents and with tortious interference claims.

For the 11 patents-in-suit, each party proposed eight terms for the Court to construe. (*See* Docket No. 142 (Joint Claim Construction Statement) at 2–3.) The parties have agreed on the construction of six additional terms. (*Id.* at 1.)

II. BACKGROUND

A. Factual Background

Fortinet sells cybersecurity products, software, and services to large institutional customers. (Docket No. 67 ("FAC") at ¶ 4.) Many of its products "provide[] network visibility to see devices connected to a network as well as the ability to control those devices and users." (*Id.* at ¶ 26.)

Forescout competes with Fortinet in that market. (*Id.* at ¶ 6.) On February 9, 2020, Forescout publicly announced a major acquisition of all its outstanding shares by Advent

International ("Advent"), a global private equity investor. (Docket No. 107 ("Countercl.") at ¶¶ 135-136.) That month, Fortinet attempted to initiate licensing discussions with Forescout. It persisted through April without success. (FAC at ¶¶ 10-12.) Then, in May, one business day before Advent's acquisition's scheduled closing, Fortinet filed this action and began a campaign to allegedly smear Forescout before its existing and potential customers. (Countercl. at ¶¶ 138-145.) Advent paused the acquisition, but eventually closed the deal on financial terms much less favorable to Forescout. (*Id.* at ¶ 146.)

B. Procedural Background

Fortinet filed suit in May 2020 for contributory, induced, and willful infringement of three patents relating to cybersecurity technology. (Docket No. 1.) Ruling on Forescout's motion to dismiss, the Court declined to invalidate Fortinet's three patents under 35 U.S.C. § 101 and found that Fortinet has sufficiently pled induced infringement. (Docket No. 55.) The Court dismissed Fortinet's contributory and willful infringement claims with leave to amend. (*Id.*)

Fortinet then filed its Amended Complaint, asserting two additional patents. (FAC.) Forescout again moved to dismiss. (Docket No. 71.) The Court declined to invalidate the two newly asserted patents' claims under Section 101. (Docket No. 94.) It also dismissed Fortinet's willful infringement claims but found induced and contributory infringement claims adequately pled. (*Id.*)

Forescout then counterclaimed against Fortinet, alleging infringement of six patents and tortious interference based on Fortinet's extrajudicial statements. (Docket No. 107.) The Court denied Fortinet's motion to dismiss the tort claims or the infringement claims under Section 101. (Docket No. 133.)

III. FORTINET'S EXPERT'S QULIFICATIONS AND OPINIONS

As an initial matter, Forescout asks the Court to disregard the declaration of Fortinet's expert, Michael Shamos, Ph.D., J.D., for three reasons: (1) Dr. Shamos "never identifies what legal standard he applied for means-plus-function claims." (Docket No. 147 ("Forescout Resp.") at 11.) (2) Dr. Shamos is not a POSITA under either party's definitions. (*Id.*) (3) Dr. Shamos's declaration accompanying Fortinet's reply brief is untimely as it came over a month after claim construction discovery had closed. (Docket No. 151 ("Forescout Sur-reply") at 8.) The Court addresses each reason below.

A. The Legal Standard Dr. Shamos Applied Is Identifiable And Reliable

Forescout first urges the Court to disregard Dr. Shamos's declarations because he fails to identify the legal standard for means-plus-function claims. (Forescout Resp. at 11.) Federal Rule of Evidence 702 requires a qualified expert to apply "reliable principles and methods" in forming his or her opinions. Fed. R. Evid. 702(c). An expert thus should identify the principles and methods applied so that the court or the jury can evaluate the expert's testimony.

Here, Dr. Shamos does not explicitly outline the legal standard for construing means-plus-function limitations in his declarations, but appears to have applied *Williamson v. Citrix Online, LLC* to his analysis. 792 F.3d 1339, 1350 (Fed. Cir. 2015). In paragraph 39 of his declaration, for example, Dr. Shamos opines, "Because 'module' is a nonce word (standing for a hardware or software component), it is possible that 'earmark provisioning module' is a mean[s]-plus-function term under pre-AIA 35 U.S.C. §112¶6." (Ex. A[1] ("Shamos Decl.") at ¶ 39.) That reasoning is consistent with the standard set forth in *Williamson*. *See* 792 F.3d at 1350 ("'Module' is a well-known nonce word that can operate as a substitute for 'means' in the context of § 112, para. 6."). Dr. Shamos's opinion therefore is distinguishable from that in the case cited by Forescout, *NetFuel, Inc. v. Cisco Sys. Inc.*, No. 5:18-cv-02352-EJD, 2020 WL 1274985, at *11 (N.D. Cal. Mar. 17, 2020). There, the court was unable to follow the expert's methodology to calculate royalty. *Id.* at *7 (finding expert's conclusion to be "impermissible black box without sound economic and factual predicates") (internal quotation marks omitted). Although Dr. Shamos should have identified the legal standard for means-plus-function limitations, his methodology is not so undiscernible or unreliable to warrant being disregarded.

[1] Exhibits A-G refer to the exhibits to the Declaration of Anthony P. Biondo in Support of Fortinet's Opening Claim Construction Brief (Docket No. 146). Exhibits H-P refer to exhibits to the Declaration of Matthew R. McCullough in Support of Defendant Forescout Technologies, Inc.'s Responsive Claim Construction Brief (Docket No. 147-1). Exhibit Q refers to the exhibit to the Declaration of Anthony P. Biondo in Support of Fortinet's Reply Claim Construction Brief (Docket No. 149-1).

B. Dr. Shamos Qualifies As A POSITA

Forescout also asks the Court to disregard Dr. Shamos's declarations because he lacks experience in network access security systems and thus is not a POSITA under either party's definition. (Forescout Resp. at 11–12.) Forescout observes that neither Fortinet nor Dr. Shamos even contends that he is a POSITA. (Forescout Sur-reply at 8.) In response, Fortinet points out that Dr. Shamos has a Ph.D. in computer science, and has taught courses in computer networking, wireless communication and Internet architecture, Internet protocols, and electronic payment systems. (Docket No. 146 ("Fortinet Br.") at 24.) Fortinet also submitted a new declaration from Dr. Shamos accompanying its reply brief setting forth the following qualifications:

> Dr. Shamos is the Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University;
>
> he has testified before legislatures on computer security;
>
> he authored an article on E-Voting Security in IEEE Security and Privacy in 2012, and was a guest editor of that issue;
>
> he authored a security analysis of the firmware of an electronic voting machine; and
>
> he supervised a graduate software project for Samsung to detect attempts to introduce malware into computer systems.

(Docket No. 149 ("Fortinet Reply") at 25; Ex. Q ("4/25/22 Shamos Decl.") at ¶¶ 6-19.)

Dr. Shamos qualifies as a POSITA under Forescout's definition. Forescout's expert, Eric Cole, Ph.D., defines a POSITA as "a person with a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cybersecurity, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields." (Ex. B ("Cole Decl.") at ¶ 19.) And "an individual with additional education or additional industrial experience could still be of ordinary skill in the art if that additional education or experience compensates for a deficit in one of the other aspects of the requirements stated above." (*Id.*)

As described above, Dr. Shamos has a Ph.D. and years of experience in computer security. Although computer security is different from network or cybersecurity, experience in the former combined with Dr. Shamos's additional education may compensate for a deficit in the latter, as Dr.

Dole contemplates. Additionally, by submitting the declarations, Dr. Shamos implicitly considers himself qualified as a POSITA under his own definition that requires "one to two years of work experience in implementing network security functions" and in "implementing network security functions." (Shamos Decl. at ¶¶ 12, 16–17, 21, 25.) Thus, Dr. Shamos implicitly acknowledges that he has experience in cybersecurity, as Dr. Cole requires.

Because Dr. Shamos qualifies as a POSITA under Forescout's definition, the Court does not disregard his opinions.

C. The Court Declines To Strike Dr. Shamos's New Declaration

In its claim construction sur-reply brief, Forescout asked the Court to strike Dr. Shamos's declaration accompanying Fortinet's reply brief (Forescout Sur-reply at 8). The sole authority that Forescout cites to support its request concerns a motion to strike an untimely expert report dressed up as a rebuttal declaration. *See Mallinckrodt, Inc. v. Masimo Corp.*, 254 F. Supp. 2d 1140, 1156–58 (C.D. Cal. 2003) (granting motion to strike 33-page "rebuttal" declaration submitted with opening claim construction brief when previously submitted expert report was rubber-stamped two-pager).

Dr. Shamos's new declaration does not appear to have prejudiced Forescout. In its sur-reply brief, Forescout criticized Fortinet for relying on that declaration for two terms. For one term, Fortinet relied on "Dr. Shamos'[s] untimely new declaration for the proposition that the preamble provides antecedent basis." (Forescout Sur-reply at 9.) But Dr. Shamos also opined so in his Claim Construction Report on the Fortinet Patents served on Forescout in May 2021. (*See* Ex. G ("Shamos Rpt.") at ¶ 77; Docket No. 146-1 at ¶ 8.) For the other term, Fortinet made arguments in the reply brief "based on Dr. Shamos'[s] untimely declaration, which relies on Figure 5" of U.S. Patent No. 9,894,034. (Forescout Sur-reply at 13.) But Forescout anticipated that argument and even included its annotated Figure 5 in its responsive brief. (Forescout Resp. at 23.) Regardless, Forescout has had an opportunity to address Dr. Shamos's new declaration in its sur-reply brief. *See, e.g.*, Forescout Sur-reply at 9 (stating that "Dr. Cole's declaration stands unrebutted" after considering Dr. Shamos' new declaration). Forescout has not shown prejudice by Dr. Shamos's new declaration.

D. Summary

In sum, the Court denies Forescout's request to disregard Dr. Shamos's declarations because Dr. Shamos is qualified, applied identifiable and reliable legal standard, and his declaration accompanying Fortinet's reply brief did not substantially prejudice Forescout.

IV. **CLAIM CONSTRUCTION**

A. Legal Standard

1. Claim Construction

"[T]he interpretation and construction of patents claims, which define the scope of the patentee's rights under the patent, is a matter of law exclusively for the court." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970–71 (Fed. Cir. 1995). Claim terms are generally given their plain and ordinary meaning, which is the meaning one of ordinary skill in the art would ascribe to a term when read in the context of the claim, specification, and prosecution history. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313–14 (Fed. Cir. 2005) (en banc). "There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Kyocera Senco Indus. Tools, Inc. v. ITC*, 22 F.4th 1369, 1378 (Fed. Cir. 2022) (quoting *Thorner v. Sony Computer Ent. Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012)).

2. Definiteness

A patent specification must "conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as [the] invention." 35 U.S.C. § 112, ¶ 2 (2006).[2] "[A] patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig*

[2] The American Invents Act (AIA) revised the pertinent provision of Section 112 to read: "The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention." 35 U.S.C. § 112(b). The revision is not substantive. The patents at issue in this case are a mix of pre- and post-AIA patents. The parties have not argued that the Court should assess their definiteness differently.

Instruments, Inc., 572 U.S. 898, 901 (2014). To comply with § 112, a patent "must provide objective boundaries for those of skill in the art." *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014). "The scope of claim language cannot depend solely on the unrestrained, subjective opinion of a particular individual." *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1350 (Fed. Cir. 2005), *abrogated on other grounds by Nautilus*, 572 U.S. at 901. The patent challenger "ha[s] the burden of proving indefiniteness by clear and convincing evidence." *BASF Corp. v. Johnson Matthey Inc.*, 875 F.3d 1360, 1365 (Fed. Cir. 2017).

3. Means-Plus-Function

"Means-plus-function" limitations generally refer to those invoking § 112 ¶ 6, now codified as § 112(f). That paragraph provides:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

35 U.S.C. § 112 ¶ 6. The overall means-plus-function analysis involves two steps.

At step one, courts "determine whether a limitation is drafted in means-plus-function format" by determining whether the limitation "connotes sufficiently definite structure to a person of ordinary skill in the art." *Dyfan, LLC v. Target Corp.*, 28 F.4th 1360, 1365 (Fed. Cir. 2022). Courts presume that "a claim limitation is not drafted in means-plus-function format in the absence of the term 'means.'" *Id.* "The presumption can be overcome if a challenger demonstrates that the claim term fails to recite sufficiently definite structure." *Id.* (citation and internal quotation marks omitted). The essential inquiry is "whether the words of the claim are understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure." *Williamson*, 792 F.3d at 1348. Such an inquiry turns on "[i]ntrinsic evidence, such as the claims themselves and the prosecution history," as well as extrinsic evidence. *Dyfan*, 28 F.4th at 1365–66.

At step two, if the limitation is drafted in a means-plus-function format, courts then "determine[e] 'what structure, if any, disclosed in the specification corresponds to the claimed function.'" *Dyfan, LLC*, 28 F.4th at 1365 (quoting *Williamson*, 792 F.3d at 1349–51). A means-

United States District Court
Northern District of California

plus-function claim is indefinite if the specification fails to disclose adequate corresponding structure to perform the claimed function. *Williamson*, 792 F.3d at 1351–52. The step one inquiry is distinct from, but "may be similar to[,] looking for corresponding structure in the specification." *Apple Inc. v. Motorola, Inc.*, 757 F.3d 1286, 1296 (Fed. Cir. 2014), *abrogated on other grounds by Williamson*, 792 F.3d at 1349.

B. U.S. Patent No. 6,363,489 (the "'489 patent")

1. "Returning An Earmark" And "Earmark Provisioning Module"

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"returning an earmark" (claim 1)	Indefinite	Plain and ordinary meaning	Plain and ordinary meaning
"earmark provisioning module" (claim 15)			Indefinite

Claim 1 recites:

> 1. A method for detecting and handling a communication from an unauthorized source on a network, the method comprising the steps of:
>
> (a) receiving the communication from the unauthorized source;
>
> (b) analyzing the communication for detecting an information gathering procedure;
>
> (c) if said information-gathering procedure is detected, indicating a source address of the communication as a suspected network reconnaissance collector;
>
> (d) ***returning an earmark*** to said suspected reconnaissance collector, such that said earmark includes specially crafted false data, and such that said earmark includes data that can serve to identify an unauthorized source;
>
> (e) analyzing each subsequent communication for a presence of said earmark;
>
> (f) if said earmark is present, indicating source address of the communication as a suspected network reconnaissance collector, and
>
> (g) if said source address is said intruder source address, applying intrusion handling procedures towards the communication from said intruder source address.

('489 patent at claim 1 (emphasis added).) Claim 15 recites:

> 15. A system for detecting and handling the communication from an unauthorized source on a network, the system comprising:
>
> > (a) An entry point to the network such that the communication passes through said entry point to reach the network;
> >
> > (b) an ***earmark provisioning module*** for preparing earmarks for sending to unauthorized source, such that said earmarks are specially crafted false data that will identify an unauthorized source;
> >
> > (c) An intrusion detection module for analyzing the communication and for detecting said earmark in the communication; and
> >
> > (d) An intrusion-handling module for handling the communication if said earmark is detected by said intrusion detection module.

(*Id.* at claim 15 (emphasis added).) Fortinet asserts that both terms are indefinite because (1) they are "highly subjective," and (2) they are means-plus-function terms that lack sufficient structure in the specification. (Fortinet Reply at 1–2.)

a. The Two "Earmark" Terms Are Not So Subjective As To Render Them Indefinite

The parties agree that "earmark" is a patentee-defined term that means (claim 15)—or includes (claim 1)—"specially crafted false data" to identify an unauthorized source. (Fortinet Br. at 5; Forescout Resp. at 2; '489 patent at 2:13-14 ("The mark is specifically crafted false data[.]").) Fortinet argues that the "specially crafted" nature of "earmark" independently renders the term indefinite because it is purely subjective. (Fortinet Reply at 2.) Fortinet's expert, Dr. Shamos, opines that the specification does not explain—and a POSITA would not understand—the difference between "false data" and "specially crafted false data." (Shamos Decl. at ¶ 38.) Forescout's expert, Dr. Cole, counters that "false data" refers to "randomly generated data" that serve no purpose, while "specially crafted false data" refer to those tailored "to identify an unauthorized source." (Cole Decl. at ¶ 32.) He points to "fake user names and passwords" as an example of "specially crafted false data" in the specification. (*Id.* (citing '489 patent at 8:23-26).)

"Earmark" is not indefinite for subjectiveness. Claim terms are "purely subjective" if "they turn[] on a person's tastes or opinion," and courts look to the written description to determine whether some standard exists to guide a person as to the scope of the claims. *Sonix Tech. Co. v. Publications Int'l, Ltd.*, 844 F.3d 1370, 1378 (Fed. Cir. 2017). Here, the claim language itself makes clear that "earmark" is not purely subjective because the false data constituting the "earmark" must be specially crafted so that they "can serve to identify an unauthorized source." ('489 patent at claim 1.) Whether false data can fulfill that purpose is objective. It does not turn on a person's taste or opinion.

Fortinet's sole authority does not support its position. In that case, the court found the term "unobtrusive manner" highly subjective because the claim language offers no objective indication of the "unobtrusive manner," and the prosecution history highlights the difficulty in pinning down the relationship between the term and the patents' embodiments. *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1372–73 (Fed. Cir. 2014). Here, in contrast, the '489 patent includes (i) guidance on what makes some false data "specially crafted," *i.e.*, they must "serve to identify an unauthorized source" ('489 patent at claim 1), (ii) how they are used, *i.e.*, they are gathered by an unauthorized user (*id.* at 2:14-15), and (iii) at least one example of "specifically crafted false data," *i.e.*, "fake user names and passwords" (*id.* at 8:23-26). These details provide guidance on how to distinguish between "specially crafted false data" and generic "false data." Fortinet thus has not proven by clear and convincing evidence that the "earmark" terms are indefinite for subjectiveness.

b. Means-Plus-Function

Fortinet separately argues that the "earmark" terms are indefinite as means-plus-function terms lacking corresponding structures. (Fortinet Reply at 1.) Absent the term "means," "returning an earmark" and "earmark provisioning module" are presumed not means-plus-function terms. *See Dyfan*, 28 F.4th at 1365. To overcome that presumption, Fortinet must show—by a preponderance of the evidence—that "persons of ordinary skill in the art would not have understood [those] limitations to connote structure in light of the claim as a whole." *Id.* at 1367.

i. "Returning An Earmark" Is Not A Means-Plus-Function Term

Fortinet argues that "returning an earmark" is a means-plus-function term because it only claims a function—to "identify an unauthorized source"—but does not recite how to craft an earmark or how it identifies the unauthorized source. (Fortinet Br. at 5.) Forescout argues that claim 1 resembles a typical method claim and "recites the acts necessary to support the specified function." (Forescout Resp. at 2.)

Although identifying an unauthorized source may be a function of an "earmark," the term "returning an earmark" recites no such function to invoke § 112, ¶ 6. Without claiming a function, even a term explicitly reciting "means" does not qualify as a means-plus-function limitation. *See Wenger Mfg., Inc. v. Coating Machinery Systems, Inc.*, 239 F.3d 1225, 1236–37 (Fed. Cir. 2001) (affirming "means defining a plurality of separate product coating zones" not subject to § 112, ¶ 6 because there was no recited function corresponding to "means"); *York Prods., Inc. v. Cent. Tractor Farm & Family*, 99 F.3d 1568, 1574 (Fed.Cir.1996) ("Without an identified function, the term 'means' in this claim cannot invoke 35 U.S.C. § 112, ¶ 6."); *Microchip Tech. Inc. v. Nuvoton Tech. Corp. Am.*, No. 19-CV-01690-SI, 2020 WL 978636, at *11 (N.D. Cal. Feb. 28, 2020) (holding "port control module" not means-plus-function limitation without recited function).

"Returning an earmark" thus is unlike the limitations in Fortinet's cited cases. Both concern terms solely describing the functions being performed. *See Advanced Ground Info. Sys. v. Life360, Inc.*, 830 F.3d 1341, 1348 (Fed. Cir. 2016) (finding "symbol generator" means-plus-function term as "it is simply an abstraction that describes the function being performed (*i.e.*, the generation of symbols)"); *Rain Computing, Inc. v. Samsung Elecs. Am., Inc.*, 989 F.3d 1002, 1006 (Fed. Cir. 2021) (finding "user identification module" means-plus-function term "because it merely describes the function of the module: to identify a user").

Even if the term claims a function, Fortinet has not shown that an "earmark" cannot connote sufficient structure. "[W]here a claim recites a function, but then goes on to elaborate sufficient structure, material, or acts within the claim itself to perform entirely the recited function, the claim is not in means-plus-function format." *Sage Products, Inc. v. Devon Industries, Inc.*, 126 F.3d 1420, 1427–28 (Fed. Cir. 1997). Fortinet presents no convincing argument that an "earmark," namely, "specially crafted false data," provides insufficient structure for Fortinet's proposed function of "identify[ing] an unauthorized source." (Fortinet Br. at 5.)

In sum, Fortinet has not shown by a preponderance of evidence that "returning an earmark" is a means-plus-function limitation. It thus is not indefinite for lacking a corresponding structure.

ii. <u>"Earmark Provisioning Module" Is A Means-Plus-Function Term</u>

Unlike "returning an earmark," "earmark provisioning module" is a means-plus-function term. At the outset, "'[m]odule' is a well-known nonce word that can operate as a substitute for 'means.'" *Williamson*, 989 F.3d at 1350. Accordingly, although this term does not recite "means" and thus is presumed not a means-plus-function limitation, that presumption is much weaker than for "returning an earmark."

The claim language does not provide sufficient structure for "earmark provisioning module"—a patentee coined term. Claim 15 only recites the function of the "earmark provisioning module," *i.e.*, preparing or creating earmarks, without explaining how to do so. Nor does the prefix "earmark provisioning" impart structure. *See Rain Computing*, 989 F.3d at 1006 (holding "user identification module" "merely describes the function of the module: to identify a user").

Forescout contends that how an "earmark provisioning module" interacts with other claim elements defines the structure of the module. (Forescout Resp. at 2.) Referring to Figure 1 (reproduced below), Forescout's expert, Dr. Cole, testifies, "a[n] [ear]mark provisioning module 22 provides false information to unauthorized source 20 and hence to the unauthorized user" that "acts as mark and enables traffic from unauthorized source 20, or even from a different unauthorized source (not shown) to be identified later if an intrusion attempt is made." (Cole Decl. at ¶ 31 (quoting '489 patent at 4:61–66).)

///

///

///

///

///

///

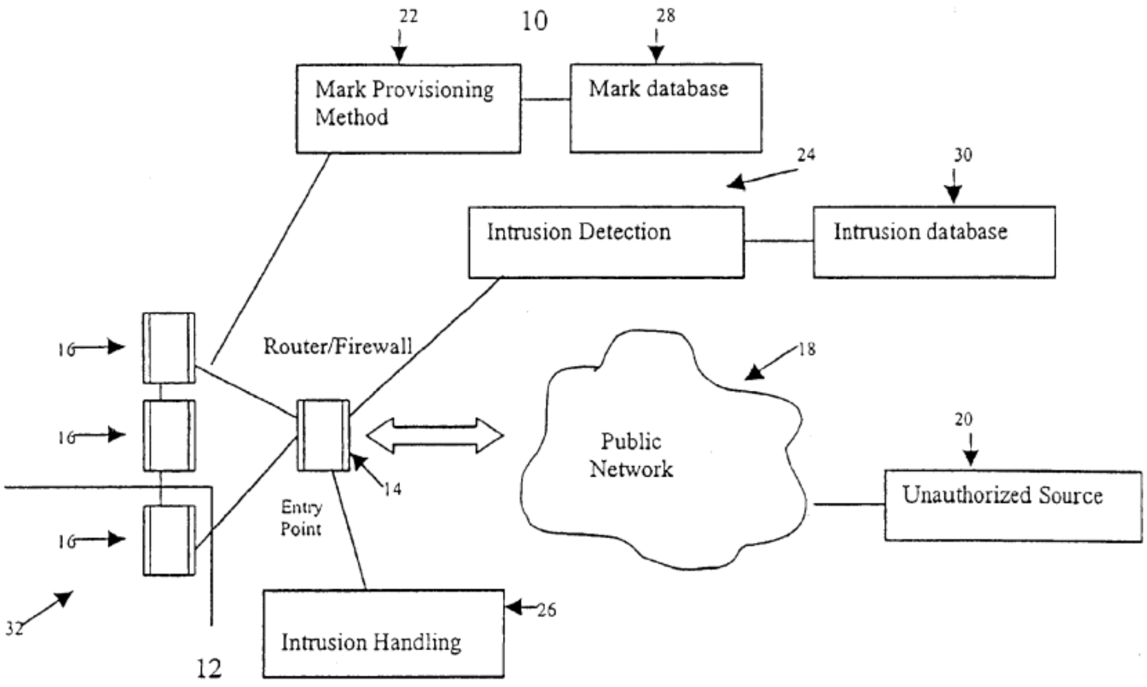


Figure 1

('489 patent at Fig. 1.) The cited specification provides "nothing more than a restatement of the function, as recited in the claim." *Traxcell Techs., LLC v. Sprint Communs. Co. LP*, 15 F.4th 1121, 1134 (Fed. Cir. 2021) (quotation omitted). Also, mere relationship with other elements alone does not provide sufficient structure. *See Media Rights Technologies, Inc. v. Capital One Financial Corp.*, 800 F.3d 1366, 1372–73 (Fed. Cir. 2015) (finding written description of "copyright compliance mechanism," including how it was connected to various parts of the system, how it functioned, and its potential functional components, was insufficient to define limitation in specific structural terms to render it a non-means-plus-function term). Forescout thus has failed to point to sufficient structure of the "earmark provisioning module."

Contrary to the specification, Forescout's counsel also suggested that the "[ear]mark database" was the structure for the "earmark provisioning module" at the claim construction hearing. (9/30/22 Hrg. Tr. at 57:9-22.) The "[ear]mark database" corresponds to box 28 in Figure 1, while the "[ear]mark provisioning module" corresponds to box 22 in the same figure. (*Compare* '489 patent at 5:22, 5:28 *with id.* at 4:57, 4:61, 4:67, 5:3-4, 5:12-13.) Hence, the "[ear]mark database" is distinct from the "[ear]mark provisioning module."

Because "earmark provisioning module" does not connote sufficiently definite structure, it is a means-plus-function term subject to § 112 ¶ 6. The Court next performs the second step to determine the structure corresponding to the claimed function.

iii. <u>"Earmark Provisioning Module" Lacks Corresponding Structure And Is Therefore Indefinite</u>

The claimed function of "earmark provisioning module" is to provide earmarks. The parties generally agree that the term means "a module that provisions earmarks." (Shamos Decl. at ¶ 36; Cole Decl. at ¶ 29 ("[T]he plain meaning of [earmark provisioning module] recites a module that creates earmarks.").)

Next, the Court needs to "determine what structure, if any, disclosed in the specification corresponds to the claimed function." *Rain Computing*, 989 F.3d at 1007. "If the function is performed by a general-purpose computer or microprocessor, then the second step generally further requires that the specification disclose the algorithm that the computer performs to accomplish that function." *Id.*

Here, the specification does not disclose a structure corresponding to the claimed function. It only describes that the module provides marks[3] "according to techniques which matches the probing method used by unauthorized users to gather information," without explaining what those techniques are. ('489 patent at 5:4-6.) It refers to the "mark provisioning method" in a single black box in a figure. (*Id.* at Fig. 1.)

Although the specification describes that modules—including the earmark provisioning module—"are installed on protected network" and "may be implemented as software, firmware, hardware or a combination thereof," it does not disclose an algorithm to achieve the claimed function of provisioning or creating earmark function. ('489 patent at 4:49-54.) In *Rain Computing*, the Federal Circuit found the claim limitation "user identification module" to be an

[3] "Earmark" does not appear anywhere in the specification, but the specification refers to "marks." Forescout contends that those are substitutes for each other. Fortinet agrees that the "earmark" of the claims may be a type of "mark." (Fortinet Br. at 6.) The Court therefore treats "earmarks" as interchangeable with "marks."

indefinite means-plus-function term. 989 F.3d at 1008. The specification provided structural examples of "computer-readable media or storage device[s]" that were linked to the function of the "user identification module"—much like the firmware and hardware disclosed here. *Id.* at 1007–08. But the court found them insufficient without an algorithm to achieve the claimed function. *Id.* The court highlighted that the fact that the "user identification module" includes software algorithms, as is the case here. *Id.* at 1008.

Likewise, in *Advanced Ground Info. Sys.*, the Federal Circuit found indefinite "signal generator," when the specification generally described that a signal was generated from certain databases—similar to the "mark database" in Figure 1 of the '489 patent—without disclosing an algorithm. 830 F.3d at 1349. The court found it not enough to "only address[] the medium through which the symbols are generated," and not the means of doing so. *Id.* Here too, the '489 patent only discloses the database through which the earmarks are generated, but not the means of doing so.

Accordingly, the specification of the '489 patent fails to disclose any structure corresponding to the recited function of "earmark provisioning module." The asserted claims containing this term are thus indefinite under 35 U.S.C. § 112, ¶ 2, and claim 15 is therefore invalid.

2. "Said Intruder Source Address"

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"said intruder source address" (claim 1)	Indefinite	The source address indicated in limitation (f)	The source address indicated in limitation (f)

Claim 1 recites:

> 1. A method for detecting and handling a communication from an unauthorized source on a network, the method comprising the steps of:
>
> (a) receiving the communication from the unauthorized source;
>
> (b) analyzing the communication for detecting an information gathering procedure;

> (c) if said information-gathering procedure is detected, indicating a ***source address*** of the communication as a suspected network reconnaissance collector;
>
> (d) returning an earmark to said suspected reconnaissance collector, such that said earmark includes specially crafted false data, and such that said earmark includes data that can serve to identify an unauthorized source;
>
> (e) analyzing each subsequent communication for a presence of said earmark;
>
> (f) if said earmark is present, indicating ***source address*** of the communication as a suspected network reconnaissance collector, and
>
> (g) if said source address is ***said intruder source address***, applying intrusion handling procedures towards the communication from said intruder source address.

('489 patent at claim 1 (emphasis added).) Fortinet argues that the disputed term is indefinite because one cannot discern with reasonable certainty whether the "source address" refers to that in limitation (c) or (f). Forescout responds that "source address" refers to that in limitation (f).

"A claim is indefinite when it contains words or phrases where the meaning is unclear, which may be the result of the lack of an antecedent basis." *In re Downing*, 754 F. App'x 988, 996 (Fed. Cir. 2018) (citing *In re Packard*, 751 F.3d 1307, 1310, 1314 (Fed. Cir. 2014)). "But the lack of an antecedent basis does not render a claim indefinite as long as the claim apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by § 112 ¶ 2." *Id.* (cleaned up). "Whether th[e] claim, despite lack of explicit antecedent basis for ['intruder source address,'] nonetheless has a reasonably ascertainable meaning must be decided in context." *Energizer Holdings, Inc. v. Int'l Trade Comm'n*, 435 F.3d 1366, 1370 (Fed. Cir. 2006).

Here, "said intruder source address" lacks an antecedent basis. The parties agree that "said intruder source address" refers to the "source address" in either step (c) or step (f). (Forescout Resp. at 13; Fortinet Reply at 3.) The Court therefore determines whether the context informs a POSITA to which "source address" the term refers.

Claim Language. The claim language indicates that "said intruder source address" refers to the "source address" in limitation (f). The claimed method is directed to "detecting and handling a communication from an unauthorized source." ('489 patent at claim 1.) To accomplish that, Forescout's expert, Dr. Cole, explains, the claimed invention indicates a "source address" as a "suspected network reconnaissance collector" that seeks to gather information in step (c). (Cole Decl. at ¶ 38.) In response, the invention "return[s] an earmark" to the "suspected reconnaissance collector." (*Id.*) Steps (e) and (f) identify the source address of the device that sends the earmark, indicating that device as an intruder. (*Id.*) Using that identified address, step (g) applies the intrusion-handling procedures if "said source address" from step (c) (the address of the suspect) matches "said intruder source address" from step (f) (the address of the intruder who attempted to use the earmark). (*Id.*) It may be argued that Forescout's reading would render meaningless the phrase "indicating source address of the communication as a suspected network reconnaissance collector" in step (f). But reading it otherwise would render redundant steps (d), (e), and (f), steps substantial and seemingly central to the patent. On balance, it is more logical to interpret "said intruder source address" as referring to "the source address" indicated in step (f).

Specification. The specification supports Forescout's interpretation. In response to "probes," *i.e.*, information gathering, from unauthorized source 20, [ear]mark provisioning module 22 provides an earmark to it. ('489 patent at 4:61-5:6.) In subsequent communications from that source, intrusion detection module 24 analyzes whether the communications include the earmark. (*Id.* at 5:14-24.) Once the earmark is identified, "unauthorized source 20 is registered in an intruder database 30," including its source address or "other intruder identifying factor." (*Id.* at 5:24-28.)

Figure 2, a flowchart of an exemplary method for probe and intrusion detection, also reflects this process. (*Id.* at 5:61-62.) Step 1 in Figure 2 corresponds to step (a) in claim 1—receiving the communication from an unauthorized source. (*Id.* at 6:6-7.) Next, the information is analyzed for "scan detection," *i.e.*, information gathering, as in claim 1's step (b). (*Id.* at 6:7-8.) Once information gathering has been detected, an earmark is returned to the unauthorized source which is also added to the intruder database. (*Id.* at 6:28-31.) "[I]f the source address is found in the intruder database . . . the unauthorized source of the packet is proactively handled as described with regard to FIG. 3." (*Id.* at 6:57-60.)

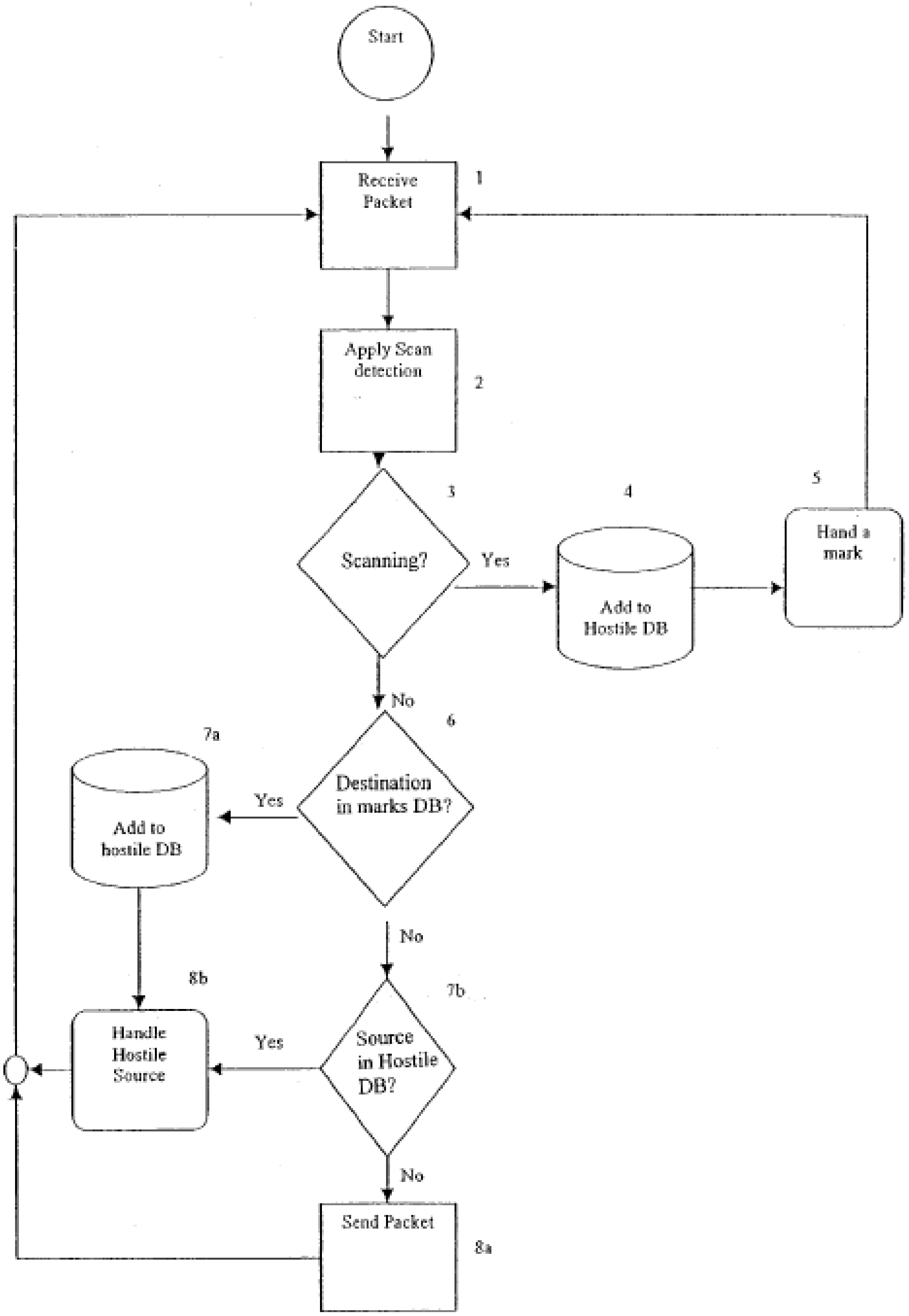


Figure 2

(*Id.* at Fig. 2.)

If "said intruder source address" in step (g) refers to "source address" in step (c), the method teaches "applying intrusion handling procedures towards the communication" once "information-gathering procedure is detected." (*Id.* at claim 1.) But that would ignore the specification that describes "provid[ing] false information to unauthorized source 20" in response to information gathering. (*Id.* at 4:61-5:6.) In contrast, if "said intruder source address" in step (g) refers to "source address" in step (f), the method teaches "applying intrusion handling procedures towards the communication" once an "earmark is present" in an unauthorized source's subsequent communication. (*Id.* at claim 1.) That reading is consistent with the specification where an unauthorized source communicating an earmark would be added to an intruder database (*id.* at 6:28-31), and "if the source address is found in the intruder database . . . the unauthorized source of the packet is proactively handled." (*Id.* at 6:57-60.).

In short, the specification supports that "said intruder source address" refers to the "source address" in limitation (f). Fortinet argues that referring to the specification is tantamount to reading an embodiment into the claim. (Fortinet Reply at 3.) But Fortinet's own authority consulted the specification, and properly so. *See Bushnell Hawthorne, LLC v. Cisco Sys.*, 813 F. App'x 522, 527 (Fed. Cir. 2020) (finding "said different IP Address" indefinite where specification provided several potential interpretations of "different IP Address").

Prosecution history. The prosecution history does not shed much light on the meaning of "said intruder source address." After the patent issued, the patentee sought correction to provide antecedent basis to the disputed term. The Examiner rejected that request, but provided no reasoning.

On balance, the broader context suggests that a POSITA would have understood the antecedent basis of "said intruder source address" to refer to the "source address" in limitation (f).

C. U.S. Patent Nos. 8,590,004 (the "'004 patent") and 9,027,079 (the "'079 patent")

1. "Dynamic Security Policy"

	Fortinet's Proposal	Forescout's Proposal	Court's Construction
"dynamic security policy" ('004 patent claim 10; '079 patent claim 10)	Indefinite	Plain and ordinary meaning	Plain and ordinary meaning

The '004 patent is directed to a method and system for controlling access to a computer network. ('004 patent at Abstract.) They do so by authenticating, and granting a certain access level to, an access point. (*Id.*) The '004 patent shares a common specification with its continuation—the ’079 patent. The relevant claims recite:

> 10. A method for regulating access to resources on a data network comprising:
>
> > receiving authentication credentials from an access point through which the client is attempting to connect to network resources;
> >
> > retrieving data from an authentication server;
> >
> > retrieving data from a ***Dynamic Security Data & Policy Database (DSDPD)***, which ***DSDPD*** includes rules indicating network resource access provisions to be applied to a given client device based on: (1) data received from the given client device indicating the compliance of the given client device with specific security policies and (2) security information said ***DSDPD*** retrieves from a network security and monitoring system (NSMS), wherein said NSMS monitors a history of network resource access authorization requests, which history includes:
> >
> > (a) identities of parties who requested authorizations; and
> >
> > (b) results of the authorization requests;
> >
> > processing the retrieved data from the authentication server and the ***DSDPD***, wherein said processing is computed according to a ***dynamic security policy***; and
> >
> > sending a response to the network access point based on the processing of the retrieved data.

(’004 patent at claim 10 (emphasis added).)

> 10. A method for regulating access via access points to resources on a data network, said method comprising:
>
> > receiving authentication credentials from an access point through which a device is attempting to connect to network resources;
> >
> > retrieving data from an authentication server;
> >
> > retrieving data from a ***Dynamic Security Data & Policy Database (DSDPD)***, which ***DSDPD*** includes rules indicating network resource access provisions to be applied to a given device based on: (1) compliance of the given device with specific security policies and (2) security information said ***DSDPD*** retrieves from a network security and monitoring system (NSMS) comprising processing circuitry communicatively coupled to the network and configured to monitor access of end systems to the network via one or more access points;

> performing a first processing of the retrieved data from the authentication server and the ***DSDPD***, wherein said first processing is computed according to a ***dynamic security policy***; and
>
> sending a response to the network access point granting the first device quarantined access to the network, based on the processing of the retrieved data;
>
> performing further compliance testing of the first device via the quarantined access;
>
> re-determining access to network resources to be granted to the first device based on results of the further compliance testing and a second processing of the retrieved data from the authentication server and the ***DSDPD***.

('079 patent at claim 10 (emphasis added).)

Fortinet contends that "dynamic security policy" is indefinite because the specifications do not explain what is "dynamic" about the security policy. (Fortinet Br. at 8–9.) Specifically, it argues that Forescout, through its expert, offers several definitions of "dynamic" and that those definitions are highly subjective. (*Id.* at 9–10.) The Court disagrees.

First, although the specifications do not expressly define "dynamic security policy," a POSITA may ascertain its meaning from that of individual words. *See Bancorp Services, L.L.C. v. Hartford Life Ins. Co.*, 359 F.3d 1367, 1372 (Fed. Cir. 2004) (declining to find term indefinite where "the components of the term have well-recognized meanings, which allow the reader to infer the meaning of the entire phrase with reasonable confidence"). The parties agree that "security policy" by itself is likely meaningful. (Shamos Decl. at ¶ 56; Cole Decl. at ¶ 56.)

Fortinet's expert, Dr. Shamos, does not dispute that "dynamic" has several well-known meanings but explains that each meaning covers a different scope. (Shamos Decl. at ¶ 56.) Forescout's expert, Dr. Cole, responds that the specifications and prosecution history support and provide guidance on the term's broad scope: a security policy may be "dynamic" by accounting for changes to a device's network provisions based on changes to that device's security policy compliance (Cole Decl. at ¶¶ 56, 57 (citing '004 patent at claim 1, 3:40-44, 9:60-10:6, '079 patent at 3:62-66, 10:15-28, Resp. to Office Action of Oct. 6, 2011)); it may be "dynamic" by requiring updates responding to the ever-changing nature of cyber security (*id.* (citing '004 patent at 3:55-

57, ’079 patent at 7:61-63)).

“[B]readth is not indefiniteness.” *BASF*, 875 F.3d at 1367. Fortinet has failed to show that Forescout’s proposed construction, though broad, falls outside a reasonable range of implementations that the claim language permits. *See Capital Sec. Sys. v. NCR Corp.*, 725 F. App’x 952, 957 (Fed. Cir. 2018) (holding “ascertains an apparent signature” not indefinite as POSITA would understand scope to include all four implementations suggested by patentee’s expert).

Second, the term “dynamic” is neither a term of degree nor a purely subjective claim phrase. Although a security policy may be “dynamic” in several ways, Fortinet has not provided evidence that whether it is considered dynamic “depends on the unpredictable vagaries of any one person’s opinion.” *Interval Licensing*, 766 F.3d at 1371 (internal quotation marks and citation omitted).

In sum, Fortinet has not shown clear and convincing evidence that “dynamic security policy” is indefinite.

2. <u>“Dynamic Security Data & Policy Database”</u>

	Fortinet’s Proposal	**Forescout’s Proposal**	**Court’s Construction**
“Dynamic Security Data & Policy Database”	Indefinite	Plain and ordinary meaning	Plain and ordinary meaning

Fortinet contends “Dynamic Security Data & Policy Database” to be indefinite for two reasons: (1) the term does not make clear what is “dynamic” about the component; (2) the claim language and specification fail to recite sufficient structure, invoking § 112 ¶ 6 and rendering the claim indefinite. (Fortinet Reply at 6.) The Court disagrees with the first reason as explained above. For the reasons below, the second reason also fails.

Absent the term “means,” “Dynamic Security Data & Policy Database” is presumed not to be a means-plus-function limitation. *See Dyfan*, 28 F.4th at 1365. Fortinet may overcome that presumption by showing that the limitation “fails to recite sufficiently definite structure.” *Id.* (internal quotation marks and citation omitted). It argues that “database” imparts insufficient structure to perform the claimed functions, including "storing data," "being 'dynamic,'" and "'retriev[ing]' security information from other components." (Fortinet Br. at 11–12.) Fortinet has failed to overcome that presumption here.

The term "Dynamic Security Data & Policy Database" does not have an obvious claimed function. The claim language simply describes what the database stores and how it operates—namely, it stores rules that specify network access provisions and security policies. (*See, e.g.*, '004 patent at claim 1 ("a Dynamic Security Data & Policy Database (DSDPD), which DSDPD includes rules indicating network resource access provisions to be applied to a given client device").) "Without an identified function, the term 'means' in [a] claim cannot invoke 35 U.S.C. § 112, ¶ 6." *York Prod.*, 99 F.3d at 1574. This is more so here where the term does not recite "means." *Cf. Microchip Tech.*, 2020 WL 978636, at *11–*12 (finding "port control module" not means-plus-function limitation term where claim did not recite any function of said module).

The two cases cited by Fortinet are distinguishable because their disputed terms clearly have claimed functions. *See Egenera, Inc. v. Cisco Sys.*, 972 F.3d 1367, 1370 (Fed. Cir. 2020) (finding claim language "configuration logic for receiving and responding to said software commands" clearly identified claimed function as the portion after the word "for"); *Synchronoss Techs., Inc. v. Dropbox, Inc.*, 987 F.3d 1358, 1367 (Fed. Cir. 2021) (noting claimed function of "user identifier module" was "identifying a user").

In sum, Fortinet did not overcome the presumption that "Dynamic Security Data & Policy Database" is not a means-plus-function term. The plain and ordinary meaning governs.

3. <u>"Dynamic Security Authentication Service Server"</u>

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"Dynamic Security Authentication Service Server" ('079 patent at claims 1, 18, 20)	Indefinite	Plain and ordinary meaning	Plain and ordinary meaning

The relevant claims recite:

> 1. A data network access security system for regulating access via

> access points to resources on a data network, said system comprising:
>
> a network security and monitoring system (NSMS) comprising processing circuitry communicatively coupled to the network and configured to monitor access of end systems to the network via one or more access points, wherein an access point is any network device adapted to provide computational devices access to the network; and
>
> a ***Dynamic Security Authentication Service Server (DSASS)*** comprising processing circuitry communicatively coupled to the network, the one or more access points, said NSMS and an authentication server external to said ***DSASS***, said ***DSASS*** including:
>
> a Dynamic Security Data & Policy Database (DSDPD), which DSDPD includes rules indicating network resource access provisions to be applied to a given device based on: (a) compliance of the given device with specific security policies; (b) security information received from said NSMS and (c) authentication information received from the authentication server
>
> an access policy module adapted to:
>
> (1) receive authentication credentials of a user, from an access point through which the user is attempting to connect to network resources using a first device,
>
> (2) cause the access point to initially grant the first device quarantined access to the network based on (i) data received from the authentication server in relation to the authentication credentials and (ii) compliance data associated with the first device received from said DSDPD;
>
> (3) after the first device has been granted quarantined access, facilitate further compliance testing of the first device via the quarantined access;
>
> (4) determine access to network resources to be granted to the first device based on results of the further compliance testing and the data received from: (i) the authentication server external to said DSASS and (ii) said DSDPD; and
>
> (5) cause the access point to grant the first device the determined access to the network resources.

(’079 patent at claim 1 (emphasis added).)

> 18. A data network access security system for regulating access via access points to resources on a data network, said system comprising:

> a network security and monitoring system (NSMS) comprising processing circuitry communicatively coupled to the network and configured to monitor access of end systems to the network via one or more access points; and
>
> a ***Dynamic Security Authentication Service Server (DSASS)*** comprising processing circuitry communicatively coupled to the network, the one or more access points, said NSMS and an authentication server external to said ***DSASS***, said ***DSASS*** including:
>
> > a Dynamic Security Data & Policy Database (DSDPD), which DSDPD includes rules indicating network resource access provisions to be applied to a given device based on: (a) compliance of the given device with specific security policies; (b) security information received from said NSMS and (c) authentication information received from the authentication server external to said ***DSASS***;
> >
> > an access policy module adapted to:
> >
> > > (1) receive authentication credentials of a user, from an access point through which the user is attempting to connect to network resources using a first device,
> > >
> > > (2) cause the access point to initially grant the first device quarantined access to the network based on data received from: (i) the authentication server external to said DSASS and (ii) said DSDPD;
> > >
> > > (3) after the first device has been granted quarantined access, facilitate compliance testing of the first device via the quarantined access;
> > >
> > > (4) determine access to network resources to be granted to the first device based on results of the compliance testing and the data received from: (i) the authentication server external to said DSASS and (ii) said DSDPD; and
> > >
> > > (5) cause the access point to grant the first device the determined access to the network resources.

(*Id.* at claim 18 (emphasis added).)

> 20. The system according to claim 18, wherein said ***DSASS*** is a Dynamic Security Authentication Service Proxy Server.

(*Id.* at claim 20 (emphasis added).)

Fortinet argues that "Dynamic Security Authentication Service Server" ("DSASS") is indefinite for several reasons. None are persuasive. First, Fortinet argues that this term invokes § 112 paragraph 6 without any corresponding structure in the specification. (Fortinet Reply at 7.)

"Dynamic Security Authentication Service Server" does not recite "means," so Fortinet must overcome the presumption that it is not a means-plus-function term. *See Dyfan*, 28 F.4th at 1365. It has not done so here. At the outset, both parties' experts agree that a POSITA would understand the term to connote the structure of a server. (Shamos Decl. at ¶ 63 ("I believe a POSITA would interpret 'Dynamic Security Authentication Service Server' as a server that provides 'Dynamic Security Authentication Service.'"); Cole Decl. at ¶ 63.) Moreover, claims 1 and 18 of the '079 patent define DSASS to "compris[e] processing circuitry communicatively coupled to the network, the one or more access points" and includes "a Dynamic Security Data & Policy Database" and "an access policy module." Although Fortinet's expert, Dr. Shamos, finds this term ambiguous because of the word "dynamic," he does not opine that the term lacks structure. (*See* Shamos Decl. at ¶¶ 58-63.) Fortinet thus has not overcome the presumption that DSASS is not a means-plus-function term.

Second, Fortinet appears to argue that DSASS is indefinite because this patentee-coined term does not appear anywhere in the specification. (Fortinet Reply at 7–8.) "There is no requirement that the words in the claim must match those in the specification disclosure." *In re Skvorecz*, 580 F.3d 1262, 1268–69 (Fed. Cir. 2009) (quoting MPEP § 2173.05(e)). The claim language itself defines the components of DSASS. And Fortinet's own expert appears to understand its meaning. (*See* Shamos Decl. at ¶ 63 ("I believe a POSITA would interpret 'Dynamic Security Authentication Service Server' as a server that provides 'Dynamic Security Authentication Service.' . . . I believe a POSITA would find 'Security Authentication Service' to likely refer to an 'authentication service for computer security[.]'").) Therefore, Fortinet has not shown by clear and convincing evidence that the term is so "insolubly ambiguous" as to render it indefinite. *Nautilus*, 572 U.S. at 911.

Finally, Fortinet again takes issue with the term "dynamic." (Fortinet Reply at 7–8.) For the same reason explained above, "dynamic" does not render this limitation indefinite.

///

///

///

D. U.S. Patent No. 10,530,764 (the "'764 patent")

	Fortinet's Proposal	Forescout's Proposal	Court's Construction
"corporate device" (claim 1)	Indefinite	Plain and ordinary meaning	"authorized device"

Claim 1 recites:

> 1. A system comprising:
>
> a memory; and
>
> a processing device operatively coupled to the memory, the processing device to:
>
> detect a connection of an endpoint device at a network switch coupled to a network;
>
> restrict access of the endpoint device to prevent the endpoint device from accessing resources of the network by applying a VLAN assignment to the network switch;
>
> establish a connection with the endpoint device;
>
> validate a client certificate corresponding to the endpoint device to authenticate the endpoint device as a ***corporate device***, wherein to validate the client certificate, the processing device to:
>
> receive the client certificate from the endpoint device, the client certificate comprising a subject name, a client public key and a digital signature of the client public key by a certificate authority;
>
> retrieve a certificate authority certificate from the certificate authority, the certificate authority certificate comprising a certificate public key;
>
> verify the digital signature of the client public key using the certificate authority public key; and
>
> verify the subject name using the client public key; and
>
> grant the endpoint device access to the resources of the network.

('764 patent at claim 1 (emphasis added).)

Fortinet argues that the term "corporate device" is indefinite "because it is fatally ambiguous." (Fortinet Br. at 16.) In Fortinet's primary authority, the claim found to be indefinite recites a step of displaying an image or images "in an unobtrusive manner." *Interval Licensing,* 766 F.3d at 1368. The Federal Circuit first found the phrase “unobtrusive manner” “highly subjective and, on its face, provides little guidance to one of skill in the art.” *Id.* at 1371. After finding the term “purely subjective,” the court looked to the written description for guidance. *Id.* The specification at issue included multiple embodiments, but it was unclear as to which embodiment the phrase related. *Id.* at 1373. The court found that even taking a narrow view of the specification and assuming that the phrase applied to only one of the embodiments, the lone example in the specification left the skilled artisan “to wonder what other forms of display are unobtrusive and non-distracting.” *Id.* A POSITA is left “to consult the unpredictable vagaries of any one person’s opinion.” *Id.* (quotation omitted).

Unlike the term “unobtrusive manner,” “corporate device” is not “highly subjective” on its face subject to “vagaries of any one person’s opinion.” *Id.* Pointing to claim language, Dr. Cole, Forescout’s expert, opines that “a POSITA would have recognized that a ‘corporate device’ is an ‘endpoint device’ that has been successfully authenticated” in accordance with the rest of the method. (Cole Decl. at ¶ 70.) That is because, he explains, the claim so distinguishes between a “corporate device” and other end point devices. (*Id.*; ’764 patent at claim 1 (“validate a client certificate corresponding to the endpoint device to authenticate the endpoint device as a corporate device”).)

The specification confirms that a “corporate device” is an authenticated device. The specification recites, “NAC agent interface 215 may receive a client certificate from NAC agent 112, which may be used to authenticate endpoint device 110 and determine whether endpoint device 110 is a corporate device.” (’764 patent at 5:29-32.) Forescout’s expert, Dr. Cole, explains that “NAC agents use claimed certificates to authenticate endpoint devices to determine whether they are a corporate device or not.” (Cole Decl. at ¶ 71.) Similarly, the specification distinguishes between “corporate devices” and “unauthorized devices” (’764 patent at 1:51-62), as well as between “corporate devices and “rogue device” (*id.* at 2:60-63). Thus, the specification teaches that a “corporate device” is an “authorized device,” rather than an “unauthorized” or “rogue” device.

Fortinet argues that Forescout’s interpretation would effectively read out the phrase “as a corporate device" from the claim, requiring only the validation of the certificate. (Fortinet Br. at 16–17; Fortinet Reply at 9.) But "surplusage may exist in some claims," *ERBE Elektromedizin GmbH v. Canady Tech. LLC*, 629 F.3d 1278, 1286 (Fed. Cir. 2010), and thus the mere fact that this claim may involve surplusage does not render the disputed term indefinite.

Fortinet also points to certain prosecution history to argue that a "corporate device" cannot simply mean any authenticated device. During prosecution, the applicant distinguished prior art for failing to disclose the "authenticate the endpoint device as a corporate device" limitation. (Ex. F at 202.) The applicant did not explain why, but the prior art appears to concern "user authentication" as opposed to device authentication. (*Id.* (prior art describing "VPN handler 68 uses the selected certificate for user authentication . . .").) The Court's construction therefore does not contradict the prosecution history.

In sum, Fortinet has not shown by clear and convincing evidence that "corporate device" is indefinite and the Court construes it as "authorized device."

E. U.S. Patent No. 10,652,116 (the "'116 patent")

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"determine a device type classification" (claim 11)	Indefinite	Plain and ordinary meaning	Plain and ordinary meaning

Claim 11 of the '116 patent recites,

> 11. A system comprising:
>
> a memory; and
>
> a processing device, operatively coupled to the memory, to:
>
> access data associated with a device, wherein the data associated with the device comprises traffic analysis data associated with the device and data received from an external system;
>
> periodically ***determine a device type classification*** for the device based on the data associated with device; and
>
> store the device type classification for the device; and
>
> apply a security policy to classified device based on the device meeting particular criteria of the security policy.

('116 patent at claim 11 (emphasis added).)

Fortinet argues that "determine a device type classification" is indefinite for two reasons. ***First***, Fortinet contends that the term does not define what a "device type" classification is, how it differs from "a classification for the device" in claim 1, and what distinguishes a categorization into groups that are based upon "device type" from groups that are not. Forescout responds that a POSITA would understand the meaning and scope of the term based on the plain meaning of each word individually, and the specification provides examples of classifying devices into groups based on the types of devices.

The term "determine a device type classification" has a plain and ordinary meaning. Fortinet's expert opines—and Forescout's expert offers no contrary testimony—that each word in the claim term has a well-understood meaning to a POSITA. (Cole Decl. at ¶ 77.)

Moreover, the specification explains that devices may be classified into "groups based on types of devices":

> A device classification heuristic may be used to classify devices into different groups. . . . The groups may be based on types of devices. For example, one group may be for devices that have a particular operating system, a second group for medical devices (e.g., a magnetic resonance imaging (MRI) device, a X-ray device, or computed tomography (CT) scanning device), and a third group for operational technology devices (e.g., device configured to detect or cause changes in physical processes through direct monitoring or control of physical devices such as valves, pumps, etc.).

('116 patent at 3:59-4:7.) The specification also describes that a device type might be grouped by how the device is connected to the network, such as by Ethernet or wireless connections:

> While it may be possible to determine certain types of identifying information (e.g., IP address, MAC address, etc.) with respect to many ***types of network-connected devices*** (e.g., those connected via a Ethernet connection or Wi-Fi™), in certain scenarios it may be difficult to determine with a high degree of accuracy certain characteristics of a particular device (e.g., whether such a device is an access point) and thereby classify the device.

(*Id.* at 2:9-17 (emphasis added).) "Because the intrinsic evidence here provides a general guideline and examples sufficient to enable a person of ordinary skill in the art to determine the scope of the claims . . . the claims are not indefinite." *Enzo Biochem, Inc. v. Applera Corp.*, 599 F.3d 1325, 1335 (Fed. Cir. 2010) (citation and quotation marks omitted).

Fortinet argues that "a device type classification" cannot simply refer to the classification of device types under its ordinary meaning. According to Fortinet, claim differentiation mandates that the disputed "a device type classification" in claim 11 must have a different meaning from "a classification for the device" in claim 1—another independent claim. Forescout responds that the patent does not have to "expressly define what is and is not a device type." (Forescout Resp. at 8.)

Fortinet fails to show that claim differentiation applies. "'[C]laim differentiation' refers to the presumption that an independent claim should not be construed as requiring a limitation added by a dependent claim." *Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006). The Federal Circuit "has declined to apply the doctrine of claim differentiation where 'the claims are not otherwise identical in scope.'" *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1238 (Fed. Cir. 2016) (quoting *Indacon, Inc. v. Facebook, Inc.*, 824 F.3d 1352, 1358 (Fed. Cir. 2016)). Fortinet does not contend that claim 1—an independent *method* claim—has the same scope as claim 11—an independent *system* claim. Fortinet's sole authority construed a term in an independent claim using dependent claims. *Karlin Tech., Inc. v. Surgical Dynamics, Inc.*, 177 F.3d 968, 972 (Fed. Cir. 1999). That is not the case here, as both claims 1 and 11 are independent claims. Claim differentiation therefore does not apply.

Fortinet similarly points to the specification to argue that "classification for a/the device" must have a different meaning from "device type classification." (Fortinet Br. at 18.) The specification has indeed used both terms in the same paragraph:

> Classification determiner 308 is configured to determine ***a classification of a device*** based on information received from one or more components (e.g., third party interface 302, agent interface 304, traffic analyzer 306, classification determiner 308, device interface 310, and network interface 312) of system 300, as described herein. Classification determiner 308 may further store ***a device type classification*** of the device. Classification determiner 308 may be configured to determine the ***device type classification*** of the device periodically.

('116 patent at 8:44-53 (emphasis added).) Fortinet's expert opines that "classification of the device" must have a different meaning from "device type classification" because the classification determiner 308 is configured to determine both. (Shamos Decl. at ¶ 72.) But that part of the specification could be consistent with the opposite conclusion that the terms mean the same throughout that paragraph. Assuming the two "classification" terms are synonymous, the specification simply describes that the classification determiner 308 can be configured to (1) determine "a classification of a device" (or, synonymously, "device type classification") ('116 patent at 8:44-45), (2) store that determination (*id.* at 8:49-50), and (3) determine that classification *periodically* (*id.* at 51-53 (emphasis added)). The specification therefore does not support Fortinet's argument that "device type classification" cannot mean "classification for a/the device."

Additionally, Fortinet argues that "the patent leaves unclear what distinguishes a categorization into groups that are based upon 'device type' from groups that are not." (Fortinet Br. at 18.) Forescout contends that "a type of device is essentially the group that it belongs to." (9/30/22 Hrg. Tr. at 84:11-12.) Forescout's contention is consistent with the Court's construction.

Second, Fortinet argues that the disputed term "is a pure recitation of function, with the closest potential structure being a generic 'processing device,' invoking § 112(f), and the specification lacks the disclosure of an algorithm for how this device type classification is made." (Fortinet Reply at 10.) In effect, Fortinet argues that a different term—"processing device"—is an indefinite means-plus-function term. Forescout points out that Fortinet did not elect "processing device" for the Court to construe. The Court agrees and does not construe it herein.

F. U.S. Patent No. 10,652,278 (the "'278 patent")

1. "Standard Based Compliance Rule"

	Fortinet's Proposal	**Forescout's Proposal**	**Court's construction**
"standard based compliance rule" (claim 1)	Indefinite	Plain and ordinary meaning	Plain and ordinary meaning

Claim 1 recites,

> 1. A method comprising:
>
> detecting, by a compliance monitoring device, a device coupled to a network in response to the device being coupled to the network;
>
> determining a classification of the device based on traffic information associated with the device;
>
> accessing a compliance rule based on the classification of the

> device, wherein the compliance rule is a ***standard based compliance rule***;
>
> performing, by a processing device of the compliance monitoring device, a compliance scan on the device based on the compliance rule;
>
> determining a compliance level of the device based on a result of the compliance scan of the device; and
>
> performing an action based on the compliance level.

('278 patent at claim 1 (emphasis added).) Fortinet argues that "standard based compliance rule" is indefinite because the term leaves open (1) what it means to be "based on a standard" and (2) what a "standard" is. (Fortinet Reply at 11.) Neither argument is persuasive.

Fortinet first argues that it is unclear whether "standard based" "requires the rule to be *defined in a language* that is standardized, or to be *implementing a rule* that is described in a standard." (Fortinet Reply at 11 (emphasis in original).) Fortinet refers to the definition of SCAP—an example of a "standard based compliance rules" ('278 patent at 2:28-31):

> SCAP is a set of open standard XML based languages for writing configuration benchmarks for computing devices. SCAP can also be used to create a benchmark of vulnerabilities that devices should not contain.

(*Id.* at 2:21-24.) "SCAP rules" is the only example of "standard based compliance rules" described in the specification. (*See id.* at 2:28-31 ("[A] device communicatively coupled to a network can be scanned using standard based compliance rules (e.g., SCAP rules) and a compliance level is computed.").)

The specification, viewed as a whole, suggests that a "standard based compliance rule" is one implementing a standard, rather than a rule written in a standardized language. First, the '278 patent—directed to "checking device compliance and remediation of device compliance issues" (*id.* at 1:7-8)—does not concern the computer language in which one writes a compliance rule. Second, the specification describes "perform[ing] compliance checks according to compliance rules of the compliance benchmark," (*id.* at 2:59-60), indicating that a "standard based compliance rule" is akin to a "benchmark" based compliance rule. Such an understanding is consistent with SCAP's purpose of creating "benchmarks for computing devices." (*Id.* at 2:21-24.) Put differently, SCAP rules are "standard based compliance rules" because they are based on benchmarks created by SCAP. Therefore, the claim and specification make clear that the term does not refer to any standardized language, but rather a rule implementing a standard.

Fortinet then argues that "there is no definitive way of telling what is and what is not a standard." (Fortinet Br. at 20 (quoting Shamos Decl. at ¶ 77).) Its expert, Dr. Shamos, explains that the "process by which a set of rules becomes a 'standard' is undefined—some 'standards' simply become de facto standards through common acceptance, although it is not clear exactly when this occurs." (Shamos Decl. at ¶ 77.) At the claim construction hearing, Forescout responds that the "standard" in the disputed term "refers to industry standards." (9/30/22 Hrg. Tr. at 35:14-15.)

Nothing in the claim or the specification limits the "standard" to an "industry standard" and neither expert so opines. Forescout's authorities do not help it. The disputed term in one case cited by Forescout explicitly recited "industry standard" and no party asserted indefiniteness. *E. Digital Corp. v. New Dane*, No. 13-CV-2897-H-BGS, 2014 WL 7139698, at *15 (S.D. Cal. Dec. 12, 2014) (construing "industry standard data storage format"). In the other case, the disputed terms refer to various specific standards by name, such as USB, ADB, SCSI, and RS-232, and standards from specific named organizations. *See Hewlett-Packard Dev. Co., L.P. v. Gateway, Inc.*, No. CIV. 04CV0613-BLSP, 2005 WL 6225388, at *1 (S.D. Cal. Sept. 7, 2005).

Nonetheless, the word "standard" has an ascertainable, ordinary meaning. Forescout's expert opines, and Fortinet's expert does not dispute, that each word of the term has a well-understood meaning to a POSITA. (Cole Decl. at ¶ 89.) Although different dictionaries offer slightly varying definitions, all suggest that a "standard" refers to an agreed-upon protocol. (*See* Dictionary of Computer Science (2016) ("A publicly available definition of a hardware or software component, resulting from international, national, or industrial agreement."); Newton's Telecom Dictionary (2016) ("standard . . . mean[s] something such as a specification established as a yardstick, gauge, or criterion by authority, custom, or general consent"; "standards" means "[a]n agreed-upon rule, regulation, protocol, dimension, interface and/or, technical specification.").) SCAP, an example of "standard based compliance rules" referred to the specification, is consistent with that definition. It is an agreed-upon "secure content automation protocol." ('278 patent at 2:20-21; *see also* Security Content automation Protocol, Computer Security Resource Center, National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/security-content-automation-protocol, last accessed on Nov. 22, 2022 ("The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas.").) A POSITA therefore can determine the scope of the invention with reasonable certainty. *See Bancorp*, 359 F.3d at 1372 (declining to find term indefinite where "the components of the term have well-recognized meanings, which allow the reader to infer the meaning of the entire phrase with reasonable confidence").

Fortinet also argues that what constitutes "standard" may change with time. (Fortinet Reply at 12.) In essence, Fortinet contends that the patent claim may cover a standard not disclosed or even contemplated in the patent. Forescout responds that the natural evolution of standards does not render the term indefinite, much like how the scope of "computing devices" changes over time. (Forescout Sur-reply at 7.) Although a "standard" may change with time, the meaning of "standard based compliance rule" does not—it always refers to a compliance rule based on an agreed-upon protocol. Fortinet's sole authority is in apposite. In *Meds. Co. v. Mylan, Inc.*, the Federal Circuit rejected a construction where, in an ongoing commercial production process, a competitor would not know whether it is *consistently* producing batches of the requisite impurity until all future batches are produced. 853 F.3d 1296, 1303 (Fed. Cir. 2017). No such ongoing process exists here.

In sum, Fortinet has not proven the disputed term to be indefinite by clear and convincing evidence. The Court accords "standard based compliance rule" its plain and ordinary meaning.

2. <u>"Compliance Level"</u>

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"compliance level" (claim 1)	"quantitative score indicating the extent to which a device is in compliance with compliance rules"	Plain and ordinary meaning	Plain and ordinary meaning

Claim 1 recites,

> 1. A method comprising:
>
> detecting, by a compliance monitoring device, a device coupled to a network in response to the device being coupled to the network;
>
> determining a classification of the device based on traffic information associated with the device;
>
> accessing a compliance rule based on the classification of the device, wherein the compliance rule is a standard based compliance rule;
>
> performing, by a processing device of the compliance monitoring device, a compliance scan on the device based on the compliance rule;
>
> determining a ***compliance level*** of the device based on a result of the compliance scan of the device; and
>
> performing an action based on the ***compliance level***.

('278 patent at claim 1 (emphasis added).) The parties primarily disagree on whether the compliance level can include a simple binary "pass/fail" as well as gradation levels. (Fortinet Reply at 13.) Forescout argues that it does, and Fortinet disagrees and construes "compliance level" as "quantitative score indicating the extent to which a device is in compliance with compliance rules."

The plain and ordinary meaning of "compliance level" does not exclude a two-level compliance. The word "level" generally refers to "a relative amount, intensity[,] or concentration." *See* Dictionary of Science and Technology (2007). Forescout's expert agrees. (*See* Cole Decl. at ¶ 84 ("[A] skilled artisan would have understood that 'compliance level' may mean any indicator showing the extent to which a device is following compliance rules, such as a (i) "high risk, medium risk, or low risk" indicator showing whether devices pose a security risk or (ii) a "Pass/No Pass" indicator showing whether a device is or is not compliant with a particular compliance rule.").) Fortinet's expert does not opine to the contrary. The Court therefore gives "compliance level" its ordinary meaning which may encompass a simple binary "pass/fail."

Fortinet observes that "*every* embodiment of or reference to a 'compliance level' in the specification is quantitative in nature," but that alone does not narrow the term's plain and ordinary meaning. (Fortinet Br. at 22–23 (emphasis in original).) Each instance in which the specification describes the "compliance level" as percentage or numerical points is in context of an example. (*See* '278 patent at 4:39-42 ("The compliance rules may have weights associated therewith thereby enabling the calculating of a compliance score or level, *e.g.*, as a percentage or a number of points."), 5:1-8 ("For example, if the compliance level is 20% or below, then operating system updates may be initiated via an update management system on the network (not shown) to attempt to update the device and increase compliance. The device may then be rescanned and upon obtaining a compliance level of 80% or above, compliance monitoring device 102 may grant the device network access."), 6:10-14 ("The compliance level can be determined based on the result of the scan according to each rule (*e.g.*, whether the device meets a condition of a rule) and a weight assigned to each rule (*e.g.*, a certain number of points or a percentage assigned to each rule)."), 6:26-30 ("For example, the first threshold may be 70 percent compliance, so a device with a compliance level that is 70 percent or above will be granted a relatively high level of network access while a device with a compliance level below the first threshold may be granted different network access, if any.").) "Such examples are 'not sufficient to redefine the term . . . to have anything other than its plain and ordinary meaning.'" *Ancora Techs., Inc. v. Apple, Inc.*, 744 F.3d 732, 735 (Fed. Cir. 2014) (quoting *IGT v. Bally Gaming Int'l, Inc.*, 659 F.3d 1109, 1118 (Fed. Cir. 2011)) (where only instances of embodiments indicating narrower construction were found in examples, holding that specification's description for "preferred embodiment" was not limiting). There is no indication that the examples in the specifications were intended to be treated as a claims limitation. The specification also discloses computing a "compliance level" (*see, e.g., id.* at 2:28-31), but that does not preclude a simple pass/fail. For example, a computed "compliance level" of 1 could indicate pass while 0 fail. The specification here therefore does not redefine "level."

Fortinet's proposed construction—"quantitative score indicating the extent to which a device is in compliance with compliance rules"—also is confusing. The word "score" typically connotes numbers, such as test scores, and "quantitative score" strengthens that connotation. But Fortinet contends that "compliance level" includes an indicator of "high," "medium," or "low" risk, which are not numerical. Fortinet justifies such inclusion because high/medium/low "expresses a comparable quantity (or *level*) of risk." (Fortinet Br. at 22 (emphasis in original).) No principled reason exists for why "compliance level" encompasses those three qualitative levels but not the two "pass/fail" levels that also expresses a comparable quantity of risk. For example, "pass" may correspond to low, and "fail" to high, security risk. Therefore, Fortinet has not overcome the "heavy presumption" that a claim term carries its ordinary and customary meaning. *Teleflex v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002).

G. U.S. Patent No. 9,369,299 (the "'299 patent")

1. "Said Network Access"

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"said network access" (claims 1, 3, 4, 8)	No construction required	Indefinite	No construction required

Claim 1 recites,

> 1. A system for out-of-band control of ***network access*** supporting multiple connections comprising:
>
> a network comprising a server device, at least one terminal device, and a communication link between them;
>
> at least one remote access device (RAD) comprising memory, and communicatively coupled to said network; and
>
> a Network Access Control Server (NACS) comprising memory, controlling ***said network access***, wherein said network access control is out of band and comprises:
>
> identity management of said connections;
>
> endpoint compliance of said connections; and
>
> usage policy enforcement of said connections;
>
> wherein said enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to its running configuration, whereby said enforcement is vendor-independent and said system is RAD-agnostic;
>
> said network access control comprising receiving a connect attempt to said network from a user device;

> said RAD authenticating connecting user to said NACS for said out of band network control;
>
> said NACS capturing RAD identification, location;
>
> restricting access to said network by said user device with a network access filter (NAF) configured on said RAD;
>
> said RAD directing said client device to an agent;
>
> on said user device, running said agent;
>
> said agent identifying client to said NACS;
>
> modifying said NAF based on compliance; and
>
> monitoring post-connection of successful connections.

('299 patent at claim 1 (emphasis added).)

> 2. The system of claim 1, wherein ***said network access*** comprises agents whereby said agents collect identity and health information about user and said RAD.

(*Id.* at claim 2 (emphasis added).)[4]

> 3. The system of claim 1, wherein ***said network access*** comprises:
>
> a VPN concentrator that is said RAD;
>
> at least one of a, Remote Access Server (RAS), firewall, intrusion protection detection system, a switch, a router, an authentication authorization and accounting (AAA) directory server, Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS).

(*Id.* at claim 3 (emphasis added).)

> 4. The system of claim 1, wherein ***said network access*** comprises a connection attempt comprising constructing a connection model from information about user and said RAD.

(*Id.* at claim 4 (emphasis added).)

> 8. The system of claim 5, wherein ***said network access*** of said connecting user device is controlled by filters based on identity and location of connecting user and said RAD.

(*Id.* at claim 8 (emphasis added).)

[4] Claim 2 is not asserted, but Forescout asks the Court to consider it for the purpose of construing the disputed term. (Forescout Resp. at 14 n.2.) Fortinet did not oppose. (Fortinet Reply at 15.)

Forescout contends that "said network access" is indefinite for two reasons. ***First,*** it argues that the term lacks an antecedent basis and "no reasonably ascertainable meaning is apparent." (Forescout Resp. at 13.) Fortinet points to the preamble as the antecedent basis. The preamble recites, "A system for out-of-band control of *network access* supporting multiple connections comprising." Forescout disagrees because the preamble refers to "network access supporting *multiple connections*" generally but not any specific instance of "network access." (*Id.* at 14 (emphasis added).)

Bushnell, Forescout's primary authority, is inapposite. 813 F. App'x at 526. The Federal Circuit there found "said different IP Address" indefinite. After noting that the term lacks antecedent basis, it found neither the claim language nor the specification clarifies which of the three classes of IP address the disputed term references—"one or more IP Addresses," "one or more second IP Addresses," or "one or more third IP Addresses." *Id.* Each potential antecedent basis "is presumed to have a separate meaning" and "presumed to refer to *different* classes of IP addresses." *Id.* (emphasis in original). Unlike that in *Bushnell*, the preamble provides the only possible antecedent basis for "said network access."

Forescout's expert, Dr. Cole, does not persuade otherwise. He opines that "[a] POSITA would ordinarily understand the term 'said network access' to apply to a specific instance of network access, *i.e.* the 'said' network access as distinguished from other network accesses." (Ex. J ("5/21/21 Cole Decl.") at ¶ 35.) He appears to have rested his conclusion on the fact that "said network access" is singular, while access to network by multiple connections should be plural. But the preamble clearly uses "network access" in singular form to refer to access by multiple connections. Forescout has not provided any intrinsic evidence why "said network access" must refer to a specific network access as opposed to "network access supporting multiple connections" generally.

Second, Forescout points to dependent claims 2, 3, 4, and 8. It observes, "the phrase 'said network access' refers to an unspecified network access (claim 1), (software) agents (claim 2), a VPN concentrator (physical device) plus one other system such as a server or firewall (claim 3), a connection attempt comprising constructing a connection model (claim 4), and is tied to a specific connecting user device (claim 8)." (Forescout Resp. at 15.) Fortinet responds that the "dependent claims just recite that 'said network access . . . comprises' various other components, much like the preamble of Claim 1." (Fortinet Reply at 15.)

Neither party's argument persuades. Contrary to Fortinet's argument, the preamble of claim 1 recites "[a] system . . . comprising" while the dependent claims recite "said network access comprises." The dependent claims thus simply do not "refer to 'said network access' in exactly the same way as independent claim 1." (*Id.*) Although Forescout may be correct that "said network access" cannot technically include all the components in the dependent claims, "[t]he dependent claim tail cannot wag the independent claim dog." *Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1360 (Fed. Cir. 2016) (citation omitted). "[T]he language of a dependent claim cannot change the scope of an independent claim whose meaning is clear on its face." *Id.* Because claim 1's preamble clearly provides the requisite antecedent basis, the Court declines to find "said network access" indefinite.

2. <u>"Said System"</u>

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"said system" (claim 11)	"said NACS"	Indefinite	"said NACS"

Claim 11 recites,

> 11. A method for out of band control for secure network access of a user device to a network comprising the steps of:
>
> receiving a connect attempt to said network from said user device;
>
> authenticating connecting user to a network access control server (NACS) by a remote access device (RAD) for out of band network control;
>
> capturing RAD identification, location by said NACS;
>
> providing out of band network enforcement comprising restricting access to said network by said user device with a network access filter (NAF) configured on said RAD; wherein said enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to its running configuration, whereby said enforcement is vendor-independent and ***said system*** is RAD-

> agnostic;
>
> directing said client device to an agent by said RAD;
>
> running said agent on said user device;
>
> identifying client to said NACS by said agent;
>
> modifying said NAF based on compliance;
>
> monitoring post-connection of successful connections.

('299 patent at claim 11 (emphasis added).) Forescout argues that "said system" appears in claim 11 without an antecedent basis and a POSITA would not know whether it refers to the "remote access device (RAD)," the "Intrusion Protection / Intrusion Detection System," the "client device," or the network access control server (NACS). (Forescout Resp. at 15–16; 5/21/21 Cole Decl. at ¶¶ 47, 50.) Dr. Shamos, Fortinet's expert, opines that claim 11 recites no other system besides NACS. (4/25/22 Shamos Decl. at ¶ 62.)

A POSITA would not understand "said system" to refer to RAD. Claim 11 describes "said system" as "RAD-agnostic." Fortinet correctly observes that "it is unclear how a RAD itself could be RAD-agnostic." (Fortinet Reply at 16.) And the claim recites "said RAD" in the same limitation as "said system," so they are "presumed to have different meanings." *Helmsderfer v. Bobrick Wash-room Equip., Inc.*, 527 F.3d 1379, 1382 (Fed. Cir. 2008).

"Said system" could not refer to the "Intrusion Protection / Intrusion Detection System." That system is not actually claimed. *Cf. In re Downing*, 754 F. App'x 988, 996 (Fed. Cir. 2018) (holding "the end user" refers to "end user" referenced in claim rather than other end users disclosed in the specification).

"Said system" also could not refer to the "client device." Nowhere does the specification disclose a client device as RAD-agnostic. To the contrary, claim 11 describe the "client device" to be "an agent by said RAD."

Having ruled out all alternative, the Court finds that "said system" refers to NACS. The specification confirms so. The claim makes clear that "said system" must be "RAD-agnostic." And the specification describes NACS as RAD-agnostic. (*See, e.g.*, '299 patent at 2:40-42 ("[T]he network access control is RAD agnostic."), 4:29-39 ("[T]he invention [a system and method for network access control] . . . is remote access device (RAD) agnostic . . . .").) The specification thus establishes that "said system" refers to "said NACS."

3. "Said System Is RAD-Agnostic"

	Fortinet's Proposal	Forescout's Proposal	Court's Construction
"said system is RAD-agnostic" (claims 1, 11)	"said NACS supports RADs from multiple vendors"	"The state of being unaffected by the manufacturer of the RAD"	"said system is unaffected by the manufacturer of RAD"

Claim 1 recites,

> 1. A system for out-of-band control of network access supporting multiple connections comprising:
>
> > a network comprising a server device, at least one terminal device, and a communication link between them;
> >
> > at least one remote access device (RAD) comprising memory, and communicatively coupled to said network; and
> >
> > a Network Access Control Server (NACS) comprising memory, controlling said network access, wherein said network access control is out of band and comprises:
> >
> > identity management of said connections;
> >
> > endpoint compliance of said connections; and
> >
> > usage policy enforcement of said connections;
> >
> > wherein said enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to its running configuration, whereby said enforcement is vendor-independent and ***said system is RAD-agnostic***;
> >
> > said network access control comprising receiving a connect attempt to said network from a user device;
> >
> > said RAD authenticating connecting user to said NACS for said out of band network control;
> >
> > said NACS capturing RAD identification, location;
> >
> > restricting access to said network by said user device with a network access filter (NAF) configured on said RAD;
> >
> > said RAD directing said client device to an agent;
> >
> > on said user device, running said agent;

> said agent identifying client to said NACS;
>
> modifying said NAF based on compliance; and
>
> monitoring post-connection of successful connections.

('299 patent at claim 1 (emphasis added).) Claim 11 recites,

> 11. A method for out of band control for secure network access of a user device to a network comprising the steps of:
>
> receiving a connect attempt to said network from said user device;
>
> authenticating connecting user to a network access control server (NACS) by a remote access device (RAD) for out of band network control;
>
> capturing RAD identification, location by said NACS;
>
> providing out of band network enforcement comprising restricting access to said network by said user device with a network access filter (NAF) configured on said RAD; wherein said enforcement is out of band and is accomplished on said RAD, comprising communicating with said RAD to make real-time changes to its running configuration, whereby said enforcement is vendor-independent and ***said system is RAD-agnostic***;
>
> directing said client device to an agent by said RAD;
>
> running said agent on said user device;
>
> identifying client to said NACS by said agent;
>
> modifying said NAF based on compliance;
>
> monitoring post-connection of successful connections.

(*Id.* at claim 11 (emphasis added).)

A patentee may act as his or her own lexicographer if the patentee "clearly set[s] forth a definition of the disputed claim term," and "clearly express[es] an intent to define the term." *GE Lighting Sols., LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014) (quotation omitted). The patentee's lexicography must appear "with reasonable clarity, deliberateness, and precision." *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1248 (Fed. Cir. 1998).

In the '299 patent, the patentee expressly defined "(vendor)-agnostic" as follows:

> Terms used in this application are described below.

> …
> (vendor)-agnostic—The state of being unaffected by the manufacturer of network devices being managed in the network.

('299 patent, 4:40–51.) The parenthesis around "vendor" suggests that this definition must cover more than "vendor-agnostic." Besides the definition of "(vendor)-agnostic," the specification only mentions "agnostic" three times: one "vendor-agnostic" (*id.* at 5:54), and two "RAD agnostic" (*id.* at 2:41, 4:36). Therefore, the definition of "(vendor)-agnostic" must relate to "RAD agnostic." In this regard, neither party advocates the swapping out "vendor" with "RAD," *i.e.*, "the state of being unaffected by RAD," presumably because NACS interacts with RAD and thus must be affected. Instead, both parties' proposed constructions of "RAD agnostic" involve RAD manufacturers. It is therefore obvious that what the system is agnostic about must be of RAD manufacturers. The Court therefore construes "said system is RAD-agnostic" as "said system is unaffected by the manufacturer of RAD."

The Court's construction addresses the parties' concerns with each other's construction. Unlike Forescout's proposal, the Court's construction is grammatically correct. It is consistent with the specification's characterization of a RAD-agnostic embodiment as a "multi-vendor solution." (*Id.* at 4:36.) It derives from patentee's express definition of "(vendor)-agnostic" and is therefore consistent with Forescout's authority that "a patentee-specified definition controls." (Forescout Resp. at 17 (citing *3M Innovative Props. Co. v. Avery Dennis Corp.*, 350 F.3d 1365, 1371 (Fed. Cir. 2003)).) It further avoids using "multi-vendor" which Forescout argues to be indefinite. (Forescout Sur-reply at 11.)

///

///

///

///

///

///

///

///

United States District Court
Northern District of California

H. U.S. Patent No. 8,458,314 (the "'314 patent")[5]

	Fortinet's Proposal	Forescout's Proposal	Court's Construction
"said template of said users and devices is associated" (claim 1)	"said templates of said users and devices are associated"	Indefinite	The Court construes the phrase of "said template of said users and devices is associated with said profile of said sponsor" as "a said template of said users and devices is associated with a said profile of said sponsor."
"said template of said endpoint" (claims 15, 20)	"said template records for endpoints"		The Court construes the phrase "said template of said endpoint is associated with said profile of said sponsor" as "a said template of said endpoint is associated with a said profile of said sponsor."

Claim 1 recites,

> 1. A method for control of computer network resources connected to a computer network supporting network endpoints by delegating control from a network administrator to at least one sponsor comprising the steps of:
>
> *creating templates* for users and devices of said computer network by said network administrator at an administrator account on a workstation connected to said computer network;
>
> creating profiles used to control said resources of said computer network;
>
> *associating said templates* with said profiles;
>
> creating at least one said sponsor by said network administrator;
>
> associating, by said network administrator, at least one of said profiles with said sponsor;
>
> delegating, by said network administrator, network management administrative privileges to said sponsor,
>
> transferring responsibility for said users and devices from said

[5] On November 15, 2022, the Patent Trial and Appeal Board ("PTAB") issued its Final Written Decision in an *Inter Partes* Review proceeding determining that all challenged claims (claims 1–13, 15–18, and 20) of the '314 patent are unpatentable. (Docket No. 173.) This encompasses all claims of the '314 patent asserted by Fortinet in this litigation (claims 1, 3, 5–8, 10, 11, 13, and 17). If affirmed, "[t]hat affirmance . . . has an immediate issue-preclusive effect on any pending or co-pending actions involving the patent." *XY, LLC v. Trans Ova Genetics*, 890 F.3d 1282, 1294 (Fed. Cir. 2018). Since Fortinet's time to appeal has not run, the Court still construes the disputed term of the '314 patent.

> network administrator to said sponsor when ***said template of said users and devices is associated*** with said profile of said sponsor; and
>
> controlling of said computer network resources by said sponsor, using said templates assigned to said sponsor by said network administrator, wherein said sponsor is constrained by said network administrator by said at least one associated profile, said sponsors not having network management administrative privileges over said network administrator.

('314 patent at claim 1 (emphasis added).) Claim 15 recites,

> 15. A system for control of network resources supporting network endpoints by delegating control from a network administrator to at least one network sponsor comprising:
>
> in a network database, *creating template records for endpoints* of said network by said network administrator;
>
> in said network database, creating at least one profile used to control said endpoints;
>
> associating *said templates* with said profiles;
>
> in said network database, creating at least one sponsor record by said network administrator;
>
> associating at least one of said profiles with said sponsor record by said network administrator;
>
> delegating, by said network administrator, network management administrative privileges to said sponsor,
>
> transferring responsibility for said endpoint from said network administrator to said sponsor when ***said template of said endpoint*** is associated with said profile of said sponsor; and
>
> by executing instructions in a microprocessor, controlling of said network resources by said sponsor, using *said templates* assigned to said sponsor by said network administrator, wherein said sponsor is constrained by said network administrator by said at least one associated profile.

(*Id.* at claim 15 (emphasis added).) Claim 20 recites,

> 20. An apparatus for control of network resources supporting network endpoints by delegating control from a network administrator to at least one network sponsor comprising:
>
> a network database containing *template records for endpoints* of said network, wherein *said template* comprises a set of rules or patterns defining scope of IT task, limitations of said endpoint and identification of an association between said endpoint and said sponsor;

> in said network database at least one profile used to control said endpoints;
>
> at least one microprocessor executing instructions associating ***said templates*** with said profiles;
>
> in said network database at least one sponsor record;
>
> at least one microprocessor executing instructions associating at least one of said profiles with said sponsor record;
>
> at least one microprocessor executing instructions delegating, by said network administrator, network management administrative privileges to said network sponsor,
>
> transferring responsibility for said endpoint from said network administrator to said network sponsor when ***said template of said endpoint*** is associated with said profile of said sponsor record of said network sponsor; and
>
> at least one microprocessor executing instructions controlling said network resources by said sponsor, using *said templates* assigned to said sponsor by said network administrator, wherein said sponsor is constrained by said network administrator by said at least one associated profile.

(*Id.* at claim 20 (emphasis added).) Claim 1 is representative of the three claims. Although claims 15 and 20 recite "template record," the parties agree that it is not distinct from "template." (Forescout Resp. at 18 n.1.)

The Court finds neither parties' construction satisfactory. Forescout argues that "said template" is indefinite because it lacks an antecedent basis and does not have a "reasonably ascertainable meaning." (Forescout Resp. at 18.) Specifically, the claims "first recite creating 'templates' plural and later recite transferring responsibility when a singular 'said template' is associated with a profile." (*Id.*) And the claims do not recite "which actor chooses the template or how that singular template is chosen from among the multiple templates created." (*Id.*) Dr. Cole for Forescout testified that a POSITA would conclude that the reference to "said template" singular has no reasonably ascertainable meaning. (5/21/21 Cole Decl. at ¶ 55.) Fortinet responds that there is no other set of templates referenced in any of the claims, so "said template" must refer to the "templates" plural. (Fortinet Reply at 18.)

The Court disagrees that "said template" singular has no ascertainable meaning. The claim language does not require differentiation among the templates plural, so "said template" simply refers to one of the antecedent templates. The claimed method broadly recites "creating templates for users and devices" and associating those templates with profiles. Whoever chooses a template from the pool of templates through whatever means does not seem to make any difference to the claimed method.

Forescout's authorities are distinguishable. In two of the three cases, the plural terms that could serve as the antecedent basis have multiple potential meanings. For instance, in *Intelligent Agency, LLC v. 7-Eleven, Inc.*, the disputed term "said reference point" could refer to multiple reference points. No. 4:20-CV-0185-ALM, 2022 WL 760203, at *33 (E.D. Tex. Mar. 11, 2022). Thus, it is unclear which reference point one should use to determine "which user among said second plurality of users has the strongest connection with said reference point" as the claim requires. *Id.* Similarly, as described earlier, the claim in *Bushnell* recites three classes of IP addresses, each presumed to have a separate meaning. 813 F. App'x at 526. The specification there in provided several potential interpretations of "different IP Address." *Id.* In *Imperium (IP) Holdings v. Apple Inc.*, the claim recited "groups of pixels, wherein each of said groups of pixels include[] a red pixel having an output" and "a first analog-to-digital converter connected to the output of the red pixel for converting the output of the red pixels . . . ." 920 F. Supp. 2d 747, 751 (E.D. Tex. 2013). The mixed use of "red pixel" and "red pixels" created an ambiguity as to "whether the outputs of multiple pixels are converted into one digital signal per pixel or are instead combined into one digital signal for all pixels." *Id.* at 757. In all three cases, the claim language requires differentiation of a singular from among the plural. As discussed above, that is not the case here.

Fortinet construes "said template of said users and devices is associated" as "said template**s** of said users and devices **are** associated." (Fortinet Reply at 18 (emphasis added).) It, in effect, changes the singular to plural in order to obtain the equivalence it asserts was clearly intended. Its own expert, however, appears to reject that construction. As Dr. Shamos opines:

> If the limitation read, "when said **templates** of said users and devices **are** associated with said profile of said sponsor," the antecedent basis would be **all** the templates created in the "creating" step, and it is unlikely that all such templates would be associated with a single profile. Therefore, the plural could not be used.

(4/25/22 Shamos Decl. at ¶ 71 (emphasis in original).)

Fortinet's authorities are not on point. *Baldwin Graphic v. Siebert* merely describes the general rule that "a" or "an" can "mean[] more than one." 512 F.3d 1338, 1342–43 (Fed. Cir. 2008). There, the court held "said fabric roll" does not mandate the singular "a pre-soaked fabric roll"—the term to which "said fabric roll" refers back. *Id.* at 1343. Here, in contrast, the referred-back term is unequivocally plural while the anaphoric phrase is singular. *Aircraft Tech Pubs. v. Avantext, Inc.* does not even concern any lack of antecedent basis. No. C 07-4154 SBA, 2009 U.S. Dist. LEXIS 105623, at *17–18 (N.D. Cal. Nov. 10, 2009).

Having found neither parties' construction satisfactory and that the claim language does not differentiate among the templates, the Court agrees with Dr. Shamos that, in this context, "the word 'a' is implied before 'said template.'" (4/25/22 Shamos Decl. at ¶ 71.) "That is, the sponsor only obtains privileges over a particular user or device when the template of that user or device has been associated with the profile of that sponsor." (*Id.*) Because the same issue exists for "said profile," the Court construes the entire phrase of "said template of said users and devices is associated with said profile of said sponsor" as "a said template of said users and devices is associated with a said profile of said sponsor," and "said template of said endpoint is associated with said profile of said sponsor" as "a said template of said endpoint is associated with a said profile of said sponsor." This construction is consistent with the structure of the patent claim's language. *Cf. Novo Indus., L.P. v. Micro Molds Corp.*, 350 F.3d 1348, 1354 (Fed. Cir. 2003) (A district court may correct an "obvious minor typographical [or] clerical" error in a patent if (1) "the correction is not subject to reasonable debate based on consideration of the claim language and the specification" and (2) "the prosecution history does not suggest a different interpretation of the claims.").

///

///

///

///

///

I. U.S. Patent No. 9,948,662 (the "'662 patent")

	Fortinet's Proposal	Forescout's Proposal	Court's Construction
"trust level" (claims 1 and 9)	Plain and ordinary meaning	"one of multiple (two or more) trust levels corresponding to the number of security features that can be disabled"	"one of multiple (two or more) trust levels corresponding to the number of security features that can be disabled"

Claim 1 recites,

> 1. A method comprising:
>
> receiving, by a network security device within an enterprise network, an application protocol request directed to an external network that is originated by a client device associated with the enterprise network;
>
> determining, by the network security device, based on the application protocol request whether a network parameter of the external network is associated with a set of trusted networks; and
>
> selectively disabling, by the network security device, application of a subset of security features of a plurality of security features to be applied to network traffic exchanged between the client device and the external network while the client device is accessing the external network when a result of said determining is affirmative, wherein the subset of security features are selected based on a ***trust level*** associated with the external network.

('662 patent at claim 1 (emphasis added).) Claim 3 depends on claim 1 and recites,

> 3. The method of claim 1, further comprising assigning the ***trust level*** to the external network, the ***trust level*** being selected from a plurality of trust levels in which a higher trust level corresponds to disabling a greater number of the plurality of security features and a lower trust level corresponds to disabling a lesser number of the plurality of security features.

(*Id.* at claim 3 (emphasis added).) Claim 9 recites,

> 9. A network security device comprising:
>
> at least one processor; and
>
> a computer-readable medium storing instructions that, when executed by the at least one processor, cause the at least one processor to perform a method comprising:
>
> receiving an application protocol request directed to an external

> network that is originated by a client device associated with an enterprise network protected by the network security device;
>
> determining based on the application protocol request whether a network parameter of the external network is associated with a set of trusted networks; and
>
> selectively disabling application of a subset of security features of a plurality of security features to be applied to network traffic exchanged between the client device and the external network while the client device is accessing the external network when a result of said determining is affirmative, wherein the subset of security features are selected based on a ***trust level*** associated with the external network.

(*Id.* at claim 9 (emphasis added).)

Forescout argues that a "trust level" must reflect more than a simple binary yes/no determination of whether a network is trusted primarily for two reasons. ***First***, Forescout argues that claims 1 and 9 recite two separate limitations relating to trust; the first—the "determining" limitation—is a simple yes/no determination, so the second limitation reciting "trust level" must reflect more than a binary choice. Fortinet responds that the "determining" step describes whether a "trust level" is assigned at all, rather than a yes/no determination. (Fortinet Reply at 20–21 (citing '662 patent at 9:48-51 ("no match is found in the trusted network parameters database, the network security device assumes that no trust level is assigned to the external network").)

The Court agrees with Forescout. The "determining" limitation recites "determining . . . whether a network parameter of the external network is associated with a set of trusted networks." ('662 patent at claims 1, 9.) Only "when a result of said determining is affirmative" (*i.e.*, a "yes" determination) do the claimed method or device selectively disable "application of a subset of security features" that "are selected based on a trust level associated with the external network." (*Id.*) Simply put, a trust level is relevant for selecting security features only after an external network is determined to be trusted. Thus, a trust level must encompass more than a trusted / not trusted determination.

Second, as Forescout observes, every reference to trust levels in the specification relates to multiple distinct trust levels. (Forescout Resp. at 20 (citing '662 patent at 8:48-52 ("A trust level to be assigned to an external network is selected from multiple trust levels, such that, a higher trust level corresponds to disabling a greater number of security features and a lower trust level corresponds to disabling a lesser number of security features."), 8:53-9:7 (example of having five trust levels corresponding to disabling different kinds and amounts of security features), 11:19-22 (An "administrator or user may be able to assign different trust levels to external networks based on their own discretion.")).)

Fortinet responds that dependent claim 3 corresponds to the embodiment with multiple trust levels, so the independent claim 1 must have a broader scope and encompass both multiple trust levels and simple yes/no determinations. Otherwise, according to Fortinet, claims 1 and 3 would have identical scopes. Not so. Claim 1 simply requires selecting a subset of security "based on a trust level." Claim 3 further explains how to do so—"a higher trust level corresponds to disabling a greater number of the plurality of security features and a lower trust level corresponds to disabling a lesser number of the plurality of security features." ('662 patent at claim 3.) Construing a "trust level" to reflect more than a yes/no determination therefore does not render claims 1 and 3 to have coextensive scopes. The Court adopts Forescout's construction.

J. U.S. Patent No. 9,894,034 (the "'034 patent)

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"initialization of a client security application" (claim 1)	"startup of the client security application"	Indefinite	Plain and ordinary meaning
"initialization of the endpoint security application" (claim 15)	"startup of the endpoint security application"		

Claim 1 recites,

> 1. A method comprising:
>
> during ***initialization of a client security application*** running on a client device:
>
> > determining, by the client security application, a network connection state of the client device with respect to a private network;
> >
> > selecting, by the client security application, a configuration for the client security application based on the determined network connection state; and

> launching, by the client security application, one or more functions of the client security application that are designated by the selected configuration to be performed by the client security application, wherein the one or more functions include one or more of web content filtering, anti-virus scanning and network access logging.

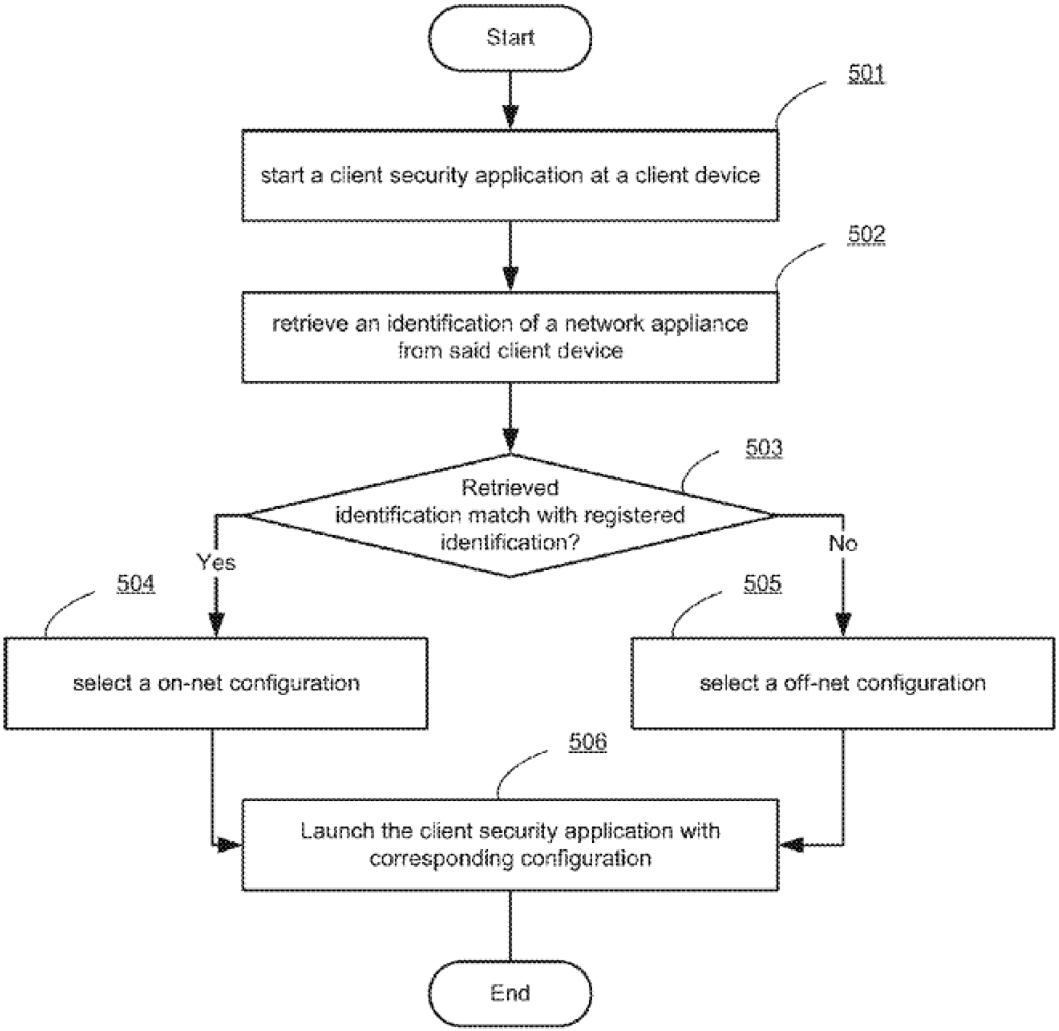
('034 patent at claim 1 (emphasis added).) Claim 15 recites,

> 15. A non-transitory computer-readable storage medium embodying a set of instructions, representing an endpoint security application, which when executed by one or more processors of a computer system, cause the one or more processors to perform a method comprising:
>
> during ***initialization of the endpoint security application***:
>
> determining, by the endpoint security application, a network connection state of the computer system with respect to a private network;
>
> selecting a configuration of the endpoint security application based on the determined network connection state; and
>
> launching, by the endpoint security application, one or more functions of the endpoint security application that are designated by the selected configuration to be performed by the endpoint security application, wherein the one or more functions include one or more of web content filtering, anti-virus scanning and network access logging.

(*Id.* at claim 15 (emphasis added).) The parties' dispute centers on the word "initialization." Forescout's expert opines that "initialization" has many different meanings to a POSITA. (5/21/21 Cole Decl. at ¶ 83.) From a user's perspective, for example, initialization of a program like Microsoft Word could be when the user clicks the icon and a loading window opens, or when a blank document opens and the user can start typing. (*Id.*) Fortinet's expert finds there to be "nothing unclear to a POSITA about the initialization process of an application." (4/25/22 Shamos Decl. at ¶ 84.) Fortinet proposes to construe "initiation" as "startup."

The specification describes "initialization" consistent with its ordinary meaning. Both experts agree that Figure 5 (reproduced below) explains a "startup procedure" ('034 patent at 8:57-58) for the client security application, including the three claimed steps in claim 1. (4/25/22 Shamos Decl. at ¶ 86; 5/21/21 Cole Decl. at ¶ 86.) From starting the application in 501 to launching the application in 506, Figure 5 describes the preparation of the client security application to perform its tasks. Further, that meaning is supported by extrinsic evidence.

Initialization generally refers to the "prepar[ation] of hardware or software to perform a task." (Webster's New World Computer Dictionary (10th ed. 2003).)


Start
501
start a client security application at a client device
502
retrieve an identification of a network appliance from said client device
503
Retrieved identification match with registered identification?
Yes
No
504
select a on-net configuration
505
select a off-net configuration
506
Launch the client security application with corresponding configuration
End

('034 patent at Fig. 5.)

The temporal connotation of "initialization's" ordinary meaning also comports with the prosecution history. During prosecution, the applicant emphasized that "initialization" is a "timing requirement. (Ex. L at 3 (distinguishing prior art because it "overlooked limitations requiring the timing of the 'determining,' 'selecting,' and 'launching' limitations to be 'during initialization of a client security application running on a client device.'").) The ordinary meaning of "initialization" has a temporal connotation because it relates to preparation of the application. The Court thus accords the disputed term its plain and ordinary meaning.

United States District Court
Northern District of California

Fortinet's proposed construction simply swaps out "initialization" for "startup," but as Forescout's expert, Dr. Cole, opines, "[t]he term 'startup' is no more clear than 'initialized.'" (5/21/21 Cole Decl. at ¶ 89.) The Court therefore declines to adopt Fortinet's construction. It also declines to find the term indefinite because the claim language provides the steps of the preparation as consistent with the ordinary meaning of "initiation."

K. U.S. Patent No. 9,503,421 (the "'421 patent)

	Fortinet's Proposal	**Forescout's Proposal**	**Court's Construction**
"security information and event management (SIEM) device" "SIEM device" "SIEM system" (claims 1, 8, 15-28)	"a device that collects logs of security events from security devices"	"a device/system that identifies and manages security threats by collecting and analyzing logs of security events"	"a device/system that identifies and manages security threats by collecting and analyzing logs of security events"

The parties agree that "SIEM" is a well-known term of art, that intrinsic evidence does not expressly define this term, and that an SIEM device is a device that collects security event information. (Fortinet Reply at 23; Forescout Sur-reply at 14.) The parties disagree whether the construction of "SIEM" must include a requirement of purpose. (Fortinet Reply at 23.) After the Court ordered the parties to further meet and confer on this term, they submitted revised definitions shown above, but the fundamental dispute remains. (Docket No. 169.)

Evidence suggests that a POSITA would understand SIEM devices to identify security threats. (5/28/21 Cole Decl. at ¶ 93.) Newton's Telecom Dictionary (28th ed. 2014) defines "SIEM" as "[t]he automated creation, updating, and analysis of event logs on an enterprise network, for the purpose of identifying problems and/or threats, and/or to fulfill a legal or regulatory requirement." (Ex. P.) Similarly, Fortinet's own website explains SIEM as follows:

> Security information and event management (SIEM) solutions collect logs and analyze security events along with other data to speed threat detection and support security incident and event management, as well as compliance. Essentially, a SIEM technology system collects data from multiple sources, enabling faster response

> to threats. If an anomaly is detected, it might collect more information, trigger an alert, or quarantine an asset.

Ex. O (https://www.fortinet.com/resources/cyberglossary/what-is-siem). Fortinet argues that Forescout plucked the definition from Fortinet's marketing material eight years after the priority date of the '421 patent. But Fortinet neither argues that the definition on its website deviated from how a POSITA would understand the term, nor contends that SIEM's definition has changed over time. The Court therefore agrees with Forescout's identified function of SIEM devices.

Although identifying security threats is "the typical purpose of an SIEM device" (Fortinet Reply at 24), Fortinet contends that it would be "improper to give weight to it" because it "is nowhere to be found in either the specification or the claims." (*Id.*) Fortinet instead relies on statement in the "Description of Related Art" that "[an] SIEM device may be deployed to collect results of the tasks performed by the security devices." (*Id.* (quoting '421 patent at 1:30-32).) Since "SIEM" is well known to a POSITA, the specification needs not describe its function. "The law is clear that patent documents need not include subject matter that is known in the field of the invention and is in the prior art, for patents are written for persons experienced in the field of the invention." *S3 Inc. v. NVIDIA Corp.*, 259 F.3d 1364, 1371 (Fed. Cir. 2001).

Fortinet objects to construing a term to include the purpose for a structure because it "has long been held to have no patentable weight." (Fortinet Reply at 24; *accord* Docket No. 169 at 1.) But the '421 patent does not claim SIEM as an invention, so no "patentable weight" needs to be given. Fortinet's authorities also do not concern claim construction. *Catalina Mktg. Int'l v. Coolsavings.com, Inc.* relates to a claim preamble's limiting effects. 289 F.3d 801, 809 (Fed. Cir. 2002) ("[P]reambles describing the use of an invention generally do not limit the claims because the patentability of apparatus or composition claims depends on the claimed structure, not on the use or purpose of that structure."). *In re Schreiber* held that prior art anticipates as long as it discloses the structure even if for a different purpose. 128 F.3d 1473, 1477 (Fed. Cir. 1997) ("It is well settled that the recitation of a new intended use for an old product does not make a claim to that old product patentable.").

Because the parties agree that SIEM devices identify and manage security threats, the Court adopts Forescout's construction.

V. CONCLUSION

The Court construes the disputed terms as explained above.

IT IS SO ORDERED.

Dated: November 28, 2022

EDWARD M. CHEN
United States District Judge